Towards Usable Cybercrime Reporting Systems through the Usability Principles : A Study in the Context of Bangladesh

by

Nowshin Nusrat Neha
21201037
Md. Ibna Sohayab
21301047
Tasfia Shobnom Anika
24341139
Omar Shahariar
24241361
Taskia Raushan Ferdousi
21201793

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
October 2025

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Nowshin Nusrat Neha
21201037

Md. Ibna Sohayab
21301047

Tasfia Shobnom Anika
24341139

Omar Shahariar
24241361

Taskia Raushan Ferdousi
21201793

Approval

The thesis/project titled "Towards Usable Cybercrime Reporting Systems through the Usability Principles: A Study in the Context of Bangladesh" submitted by

1. Nowshin Nusrat Neha(21201037)
2. Md. Ibna Sohayab(21301047)
3. Tasfia Shobnom Anika(24341139)
4. Omar Shahariar(24241361)
5. Taskia Raushan Ferdousi(21201793)

Of Fall, 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October, 2025.

Examining Committee:

Supervisor:
(Member)

Dr. Farida Chowdhury
Professor
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Dr. Jannatun Noor Mukta
Associate Professor
Department of CSE & Director
Data Science Program
United International University

Thesis Coordinator:
(Sign)

Md. Golam Rabiul Alam, PhD
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Reporting is crucial in preventing cybercrimes, but most crimes perpetrated online go unreported to the authorities. As a result, various types of cyber crimes, like identity theft, hacking, bullying, cyber threats, and so on, are not investigated, and the attackers remain unpunished in Bangladesh. However, some online portals are available for raising awareness about and reporting cybercrimes in Bangladesh. Some of the websites include the Criminal Investigation Department (CID), Bangladesh Telecommunication Regulatory Commission (BTRC), Digital Security Agency (DSA), and others. Bangladesh also has an Android mobile app called 'Online GD', which covers every police station in the nation. The websites are challenging to navigate, have an unresponsive design, and have inadequate security measures, which is the main reason behind the lack of acceptance of online reporting in Bangladesh. To support this assertion, a structural heuristic study was conducted on these systems, and we found that many features, including authenticated registration and login, an easy-to-find complaint form, and user-friendly UX, are not present in these portals. The websites and the app are not very user-friendly, and they are not handled adequately by Bangladesh's law enforcement. To gain more insight, a moderated usability evaluation (40 participants) was conducted. From this study, it was found that major usability factors like easy navigation, findability, and complaint forms were missing. Users were not very comfortable trusting and using these systems. Furthermore, to gain knowledge about how the law enforcement of Bangladesh actually handles these systems, a semi-structured interview study (5 administrative personnel) was also administered on these systems. By analyzing these data through thematic analysis, it was established that although a lot of users do prefer online reporting systems over physical reporting, due to the scarcity of better usability in online reporting systems, they refrained from using them due to a lack of trust and usability. A well-versed, user-friendly UX prototype website was proposed and tested using Simplified Usability Questionnaire (SUS) and Affective Technology Interaction (ATI) evaluation, to ensure better usability and increase use of online reporting in Bangladesh. This study aimed to enhance the efficiency and effectiveness of online cybercrime reporting in Bangladesh by improving its usability and accessibility.

Keywords: Usability issues; Human-Computer Interaction; Cybercrime Reporting; Cyber threats; Criminal Investigation Department (CID); Bangladesh Telecommunication Regulatory Commission (BTRC); Digital Security Agency (DSA); Online GD app; User friendly platform; Human-Computer Interaction; Platform design; Qualitative methods; Thematic Analysis; Simplified Usability Questionnaire (SUS); Affective Technology Interaction (ATI)

Table of Contents

Chapter 1

Introduction

Cybercrime has emerged as a severe problem in the world, and in the case of Bangladesh, the speedy advancement of internet facilities has provided new avenues for criminal activities. Despite reported platforms being easily accessible, navigating through these sites' portals presents a challenge to the users because of issues of usability and user experience design that are always present when it comes to online platforms. Eradicating this challenge requires using principles in Human-Computer Interaction (HCI), making cybercrime reporting systems more efficient. This thesis aims to improve an existing online cybercrime reporting portal in the form of a Website following local HCI guidelines regarding Bangladesh. The usability of current cybercrime reporting systems in Bangladesh faces several challenges like complicated interactions, absence of usability, and language issues. This tends to deter users from reporting incidents and delay the efforts of law enforcement agencies in fighting cybercrime. Therefore, we aspire to recast these systems based on features that are easy to invoke, understandable, and simple to navigate so that as many people from across different strata of society can report cybercrime cases. This development will be carried out under the guidance of HCI principles, and user feedback, task completion, and system learnability will be adopted. The importance of this research is quite apparent. Information technology-based crimes pose threats to individuals, companies, and the government systems. A user-friendly and effective reporting system can enable users to report events faster and enable authorities to come in swiftly. Furthermore, considering HCI principles brings about an efficient understanding of the users' needs in the system, thus enhancing user satisfaction and system interest. Technological fairness in Bangladesh is different; it is necessary to design a system where everyone can get comfortable, from advanced users to complete outsiders of the technological environment. This research aims to answer the following research questions in detail, specifically noting the application of Human-Computer Interaction (HCI) techniques to enhance the usability of cybercrime reporting portals in Bangladesh. It is meant to discover the frequently encountered problems when using existing reporting platforms and understand how its changes can provide an equal experience to users regardless of their IT literacy. The primary goals of this thesis are to discover usability issues in existing systems, develop a new and improved cybercrime reporting web portal and assess the usability, accessibility, and satisfaction with the new system. Through this, the research wants to develop a more friendly and efficient platform for target users in Bangladesh.

1.1 Background and Motivation

Cybercrime has escalated globally, and the increasing speed of internet access in Bangladesh has also increased chances of online fraud, identity abuse, harassment, and extortion. In turn, a number of government-controlled access points (e.g., CID, BTRC, DSA portals and the Online GD app)[1] [2] [3] [4] have been added to facilitate reporting. But, the citizens continue to have difficulty with (i) finding the right channel through which to present their issue, (ii) knowing what should be presented and (iii) monitoring what occurs upon submission - resulting in the issue being deserted, an additional filing and little trust. In earlier research of e-government and government systems, these failures have been found to be frequently based on usability and communication issues instead of technology: confusing information structure, jargon, poor language support, poor feedback/confirmation, inaccessible mobile interfaces have been shown to routinely compromise completion and follow-through [5], [6]. Disconnected work flows among the agencies and absence of an integrated status-tracking system even in low resource and mixed-literacy settings like in Bangladesh further slows down the time-to-action and deteriorate the quality of evidence.

Simultaneously, HCI and usable-security literature may provide explicit principles and tools that can make reporting journeys better when implemented on an end-to-end basis. Heuristic testing is an effective way to uncover system-wide interface problematic areas (additional navigation, consistency, error prevention, displaying the state of the system) [5], [7]; predefined tools like the System Usability Scale (SUS) are useful in measuring perceived usability and improvement over time [8]; and user-centered design patterns (plain-language prompts, gradual disclosure, inline validation, displaying the status of the system) contribute to higher rates of completion and a reduced number of avoidable errors [6]. Nevertheless, a lot of previous work does not go beyond recommendations or one-method audits. There is little research comparing expert review and task-based user testing and stakeholder interviewing in the same program and even less of the literature generalizes its results to a working locally constrained prototype that is tested against existing systems in real world settings.

This thesis discusses such gaps. To begin with, it identifies tangible problems in usability and work-flow along the reporting channels that Bangladeshis would most probably resort to. Second, it incorporates the view perspectives that typically are in siloed, such as experts (heuristics), citizens (task performance and feedback), and frontline officials (operational constraints such as identity verification limits, cross-agency handoffs, and data-sharing barriers).Third, it transforms that evidence into a usable, HCI-informed web prototype designed to address the context of Bangladesh, to focus on the discoverability, guided evidence capture, trustful authentication and transparent case tracking; and evaluates the results with standardized measures (e.g. SUS) as well as the qualitative feedback [5], [8]. The work will increase the success of reporting, maintain the quality of evidence, and decrease administrative workload that the prior guidelines have not always managed to do by transitioning to diagnosis to tested design [6].

1.2 Existing Cybercrime Reporting Systems

There are four main and government-operated entry points to cybercrime awareness and reporting in Bangladesh, which are the Bangladesh Telecommunication Regulatory Commission (BTRC) site, the Criminal Investigation Department (CID) site, the Digital Security Agency (DSA) site, and the Online GD mobile app [1] [2] [3] [4]. We chose them due to the visibility, official sanction, and end-to-end nature of the citizen journey (formatting and guiding to police intake); and to the modality and constraints differences between informational web pages and form-intensive flows (desktop and Android), we can identify where we are experiencing channel-specific and system-wide problems. On the face of it, BTRC and DSA offer guidance and direction of complaints, CID offers information on police service and access to digitalized mechanisms, and Online GD offers a mobile front door to the process of making General Diary entries that citizens are increasingly considering as a means of cyber incident.

In order to measure these touchpoints, we have used a three pronged HCI assessment. First, trained evaluators came up with recurring interface and content problems relative to principles of design (visibility of system status, match to user language, error prevention and recovery, consistency and standards) [5], [7]. Second, practical failure of navigation, evidence submission and authentication, and follow-through in task-based usability testing with target users was identified and perceived usability was measured using standardized usability tools, including SUS [8]. Third, stakeholder interviews with law-enforcement and others involved in the process demonstrated that there are operational bottlenecks in place that limit the nature of identity-verification, handling of evidence, multi-tier handoffs, and barriers to data sharing that define the extent to which public-facing systems can practically accommodate [6]. Such combination addresses gaps that have been repeatedly identified in literature on e-government and usable-security domains to low-resource and mixed-literacy environments: confusing information architecture, use of jargon, limited language support, weak confirmations/status, mobile friction, and discontinuous inter-agency workflows slowing down time-to-action and reducing evidence quality. The selection of BTRC, CID, DSA, and Online GD therefore grounds all further analyses: heuristic results are synthesized by evidences of user-testing to form explicit design requirements and checked by the reality of the operations as revealed in interviews, making a trace between the four existing systems and requirements and a working prototype and ensuring that the resulting recommendations are as user-centered as possible and institutionally feasible [5], [6], [8].

1.3 Problem Statement

Although various formal reporting methods exist in Bangladesh regarding cybercrime (e.g., BTRC, CID, DSA, or the Online GD application) [1] [2] [3] [4], citizens still have a challenging reporting process, which is hard to find, hard to fill, and hard to trace. Earlier HCI and e-government studies have always cited such failures as being in part due to a lack of technology, but in fact to a lack of usability and coordination, bewildered information architecture, content heavy in jargon, poor

status/feedback, weak authentication, and to inter-agency workflows that are not well coordinated and as such undermines evidence and causes delay to action [5], [6], [7], [9]. Although traditional (heuristic assessment, task-based testing, standardized measures such as SUS) methods are well-reported [5], [8], little of the literature goes beyond a guideline or one-method audit and seldom goes the extra mile to have a validated redesign in a low-resource and mixed-literacy environment.
The gaps in the literature and practice, which were observed, are discussed here briefly:

1. **Lack of end-to-end perspective :** Within most studies, pages or forms are audited, but few of them relate citizens facing failures to limitations in the back office (identity check restrictions, multi-level handoffs, cross-agency data sharing) and thus few recommendations are operationalizable [6]

2. **Absence of triangulation :** Triangulated research involving expert heuristics and user testing and stakeholder interviews are rare; however, single-method research is prevalent [5], [8].

3. **Lack of focus on the inclusive design :** In mixed-literacy, multilingual, mobile-first settings, the features of evidence capture (links, screenshots, timestamps), error recovery, and plain-language prompts are not specified, lowering the completion and the quality of reports [9].

4. **Feedback and continuity gaps:** It does not support feedback and continuity feedback consistently and encourages users to submit multiple copies of a filing and undermines trust [6].

5. **Guidance to validated redesign:** Lots of works present principles; few provide the functioning prototype that is adjusted to the local constraints and compared with the existing systems using standardized metrics (e.g. SUS) and qualitative evidence [8].

The usability-trust-coordination gap that persists in the ecosystem of cybercrime reporting in Bangladesh is that citizens are unable to reliably discover, fill in, and follow up online reports, and institutions unable to effectively verify, triage, and respond to them. This is because the available interfaces and workflows are not designed and tested to accommodate low-resource mixed-literacy realities. The field does not have an end-to-end, empirically based redesign that (i) is based on triangulated evidence (heuristics, user testing, stakeholder interviews), (ii) operationalizes the patterns of inclusive HCI to capture evidence, authenticate evidence, and provide feedback, and (iii) can be verified against the status quo using standardized instruments and qualitative output [5], [6], [8].

Such a gap is bridged by this thesis by establishing actual failures of the four most-used channels, interpreting them into practical, locale-sensitive design specifications, implementing a web prototype in the real world, and rigorously testing it to demonstrate some measurable usability, trust, and administrative improvements.

1.4 Research Objectives

This research aims to solve the current problems around the effectiveness of existing cybercrime reporting systems in Bangladesh and the utilization of HCI principles to measure the level of trust and satisfaction of the users towards the modified system. The following objectives guide the study to achieve these goals:

1. To identify and analyse the key usability problems confronted by users while employing current reporting services against cybercrime including CID, BTRC, DSA, and the 'Online GD' mobile applications.

2. To explore the extent of tech challenges that hinder users, including OTP problems, non-friendly interfaces as far as reporting cybercrimes is concerned.

3. To recognize the user needs, particularly with regard to low literacy level users and to develop interfaces for the improvement of attractiveness and usability of the cybercrime reporting platform for all users.

4. To determine how principles of HCI can be employed to design and incorporate useful features that will enhance the usability of cybercrime reporting interfaces.

5. To evaluate the degree of effectiveness of the redesigned platform in terms of credibility and urging users to report cybercrimes, especially in cases when the incidents are not as well-reported.

6. To measure the comparison of the newly designed platform with other systems that have already been developed for reporting cyber crimes in Bangladesh as well as to get more information about necessary improvement for increasing user satisfaction.

1.5 Research Questions

Users of cyberspace in Bangladesh, who become victims of cybercrime, experience a range of usability problems when engaging with online reporting systems including CID, BTRC, DSA,the 'Online GD' application. While these platforms are helpful in these cybercrime matters, the general experience is lacking in multiple ways as far as usability, accessibility, and user-orientation for users of different levels of technical expertise. The research aims to investigate these issues and tries to answer the following research questions:

1. **RQ1:** What are the key usability challenges faced by cybercrime victims or regular citizens in Bangladesh when using existing online reporting platforms like the Criminal Investigation Department (CID), Bangladesh Telecommunication Regulatory Commission (BTRC), Digital Security Agency (DSA), and the "Online GD" mobile app?

2. **RQ2:** How can the portal be structured to address the needs of a broad range of users, including low levels of digital literacy users?

3. **RQ3:** How can the law enforcement of Bangladesh resolve the technical shortcomings, operational mechanisms, and user engagement strategies of the existing cybercrime reporting system to enhance trust, accessibility, and a general working system for both the users and the law enforcement?

4. **RQ4:** What are the HCI principles that could be used in redesigning digital systems to deal with technical problems and incorporate user-friendly interfaces which will provide user trust, motivation and satisfaction than the current cybercrime reporting systems in Bangladesh?

5. **RQ5:** Can higher usability of digital systems increase the acceptance of online applications, or are there other reasons behind not having higher adaptability of these systems?

1.6 Research Contribution

This thesis provides six intersecting contributions in which it advances towards diagnosis to a validated design of cybercrime reporting in Bangladesh:

1. **Evidence-based diagnostic of current channels :** A systematic evaluation of four government-run entry points consisting of BTRC, CID, DSA, and the Online GD app consisting of an expert heuristic assessment, task-based user testing, and stakeholder interviews.The result is an all-encompassing map of usability, accessibility, and breakpoints in the workflow (discoverability, language and terminology, evidence capture, authentication, status/feedback, and cross-agency handoffs) that will respond to the query why it is so difficult to file with the state and why it is so difficult to take action with the government.

2. **Problem-to-requirements trace based on HCI :** We map the above breakdowns into design requirements that can be implemented as per the HCI principles (visibility of system state, correspondence to the language of the users, error prevention/recovery, consistency, and gradual disclosure). All requirements can be linked to either one or multiple empirical results, so the recommendations do not consist of generalized guidelines, but rather the reactions to identified pain areas and operational limitations.

3. **A locally similar, user-friendly web portal :** We have an operational reporting platform which is designed in a mixed-literacy, mobile-first environment in Bangladesh. They are problem-led entry with guided evidenced capture (links, screenshots, timestamps) layered and trusted verification and transparent tracking of cases with user initiated follow-ups- whilst sorting the submissions to be viewed by administration (normalized fields, preserved metadata, deduplication cues).

4. **Comparative usability analysis of the suggested design :** With standardized measures (e.g., SUS) and task performance measures, we will be able to compare the prototype to the existing systems and obtain quantitative data of perceived usability, task success and user confidence. The qualitative feedback should supplement the metrics to display the residual friction and

potential for iteration and give a strong foundation on which to make adoption decisions.

5. **Guidance on operations and policy recommendations :** Practice-sensitive advice on limits to verification, handling of evidence, routing of cases, and sharing of information between agencies (including social platforms and financial institutions) are obtained during interviews with law-enforcement and related institutions. We combine these into organizational and policy suggestions (e.g., role-based case management, formal MOUs/APIs, training and resourcing) which render the UX improvements institutionally tenable.

6. **Reuse and replicate artifacts :** We contribute (i)an annotated set of evaluation tools and task scripts, (ii) a coding scheme of themes and sample visualizations generated during the course of interviews (e.g., interviewee-theme heatmaps), and (iii) a set of requirements checklist that may be adapted and customized to test and redesign reporting flows of similar, under-resourced, multilingual settings.

This thesis connects citizen experience to the administrative reality in order to demonstrate how HCI-inspired methods could turn the assemblage of portals into a single, believable experience of reporting that would enhance reporting success and prevent the dissipation of the quality of evidence and reduce the burden on the back-office, and also provides a measurable, assessed path to government deployment.

1.7 Structure of the Thesis

This thesis is organized into several chapters to systematically address the research objectives and findings. Chapter 1 introduces the background of the study, outlining the motivation behind the research, identifying the existing gaps in cybercrime reporting systems, and defining the research questions, objectives, and contributions. Chapter 2 provides an in-depth literature review on the literature concerning current reporting systems in cybercrimes in Bangladesh and internationally, their limitations, and the research gap that this thesis seeks to fill.

Chapter 3 details the research methodology, including the selection of participants, data collection methods, and the evaluation processes used, such as heuristic evaluation, user testing, and semi-structured interviews. Chapter 4 presents the results of usability testing conducted on existing government cybercrime reporting platforms, including the CID, BTRC, DSA, and the Online GD mobile app. The findings identify key usability issues and provide insights into the users' experiences.

In Chapter 5, the results of heuristic evaluations are discussed, focusing on usability issues mapped to Nielsen's heuristics. Visual summaries are provided to illustrate the severity of usability patterns across the platforms. Chapter 6 outlines the interview study with law enforcement and other stakeholders, summarizing the operational and technical challenges they face and providing recommendations for improvement.

Chapter 7 introduces the proposed redesigned cybercrime reporting website, detailing the design rationale, the technologies used, and key features that incorporate the findings from previous chapters. Chapter 8 evaluates the usability of the proposed system through user testing, comparing it to existing platforms and presenting metrics such as the System Usability Scale (SUS) and Affective Technology Interaction (ATI). Chapter 9 discusses the implications of the findings for Human-Computer Interaction (HCI) and public-sector service design, reflecting on the process and methodology used in the study. Finally, Chapter 10 concludes the thesis, summarizing the contributions of the research, discussing its limitations, and suggesting avenues for future work.

Chapter 2

Literature Review

This chapter conducts an extensive examination of cybercrime reporting systems within and outside Bangladesh through literature study. The research seeks to judge the operational quality of existing reporting channels and locate the problems that prevent them from working optimally. A review has been conducted through academic papers and articles and journals to build fundamental knowledge about current system performance and limitations. The article investigates how government organizations like the Criminal Investigation Department (CID) and Bangladesh Telecommunications Regulatory Commission (BTRC) and Digital Security Agency (DSA) process reports of cybercrime.

This chapter evaluates reporting platform usability defects together with authentication barriers and accessibility levels to determine the main causes behind ineffective cybercrime operations. Research conducted in this chapter will create an improved reporting system that enhances security measures and vulnerability access strategies for Bangladesh's cybercrime victims.

2.1 Background

Our thesis outlines the structure of better reporting system that will enable Bangladeshi citizens and give a chance to the victims of cybercrimes to report incidents effectively. In this case, we have considered academic papers, articles and journals in order to make an analysis of what is commonly available. This has shown that one of the issues that make the management of incidence of cybercrime a difficult problem is the poor intervention by police. The denunciation of such incidences is complicated for the victims. The reporting system is mainly an online web or application-based portal where people can simply reach out for help, concerning cyber attack or any offense committed on them and thus the law enforcing authorities will take necessary actions. The chief objective of these reporting systems is to expedite the reporting process for the occurrence so that people do not have to physically approach the police stations to file an FIR. Affected persons are able to open a profile where they can upload their testimony or/and other evidence in relation to the crime they fall victims of, and the police will be directly addressing the submissions. Bangladesh does have some online reporting websites available those are: These agencies are the Criminal Investigation Department (CID), Bangladesh Telecommunications Regu-

latory Commission (BTRC) and the Digital Security Agency (DSA). Still, these systems lack easy, natural interaction capabilities. We discovered that there are problems of usability with the existing websites, such as during submission, there was no proper authentication of the users; since fake reporting can also pose a problem. On some of the websites there were no other sections where victims could post evidence of the crimes committed. Our intended changes include improving the reporting system and creating a better website for online reporting of cybercrimes in Bangladesh.

2.2 Related Works

This section gives a detailed analysis of the major topics and factors on the cybercrime and cybercrime management. It starts with cybercrime in the context of Bangladesh. Also, its local characteristics, problems and the efficiency of the existing reporting systems. It is then followed by an analysis of cybercrime reporting frameworks in other countries. It also assesses the financial components of cybercrime and the neighboring region of India for larger economic context. Alongside this, the level of awareness about cybercrime and ways to protect is emphasized as a critical component of public knowledge and behavior. Finally, the gaps in the laws and policies which impact on cybercrime handling are recognised and this section provides the basis for identifying the important avenues for which more research and development is required.Through this sequential analysis, the research gap is clearly framed, guiding the focus and objectives of the current study.

2.2.1 Cybercrime in the context of Bangladesh

M. S. Rana [10] focused on the types of cybercrime occurring in Bangladesh and its impact on individuals, businesses, and the economy. The author reviews some exciting literature on cybercrime. The effectiveness of the current legal framework in tackling cybercrime is discussed in this study. They collected data by interviewing experts and surveys. The overall dataset is qualitative. The author explores different types of cybercrime like hacking, malware, cyberbullying and harassment, identity theft, online fraud, data breaches, etc. Over 71% of people in Bangladesh have a Facebook account, and that's why Facebook is highlighted as the most prominent platform where cybercrimes, such as online fraud and identity theft, frequently occur. In this paper, the author also discusses the challenges in law enforcement, including the lack of resources, training, and specialized legal frameworks. To reduce cyberattacks in Bangladesh, the author recommended some practical steps, including establishing a dedicated cybersecurity task force, strengthening legal frameworks, enhancing public awareness and education, investing in cybersecurity infrastructure, training law enforcement, and encouraging reporting and support systems.

Rony et al. [11] focused on investigating the experiences of young adult users in urban Bangladesh regarding cybercrime and how they handle this kind of situation. This paper identified several problems related to cybercrime in Bangladesh. The authors of this paper used mainly qualitative research methods. They conducted semi-structured interviews and group discussions with 23 young adults. From this, they find out that the main issue regarding handling cybercrime among young adults

is the need for more trust in government security systems. 61% of young participants who took part in this research showed skepticism towards government agencies. The authors have also collected data from two primary sources: the Cyber Security and Crime Division of the Dhaka Metropolitan Police and the Cyber Tribunal of Bangladesh. The authors have also gathered data from interviews with police officers and public prosecutors. After the research, the proposed solution was to increase awareness and education about cyber safety among young adults. However, this paper does have some research gaps. For example, the authors highlighted that many users need to be fully aware of the vulnerabilities they face. This critical area requires more exploration.

N. M. Zawad [12] discussed cyber-attacks, the rise in cyber crimes, and human rights concerns in the context of Bangladesh in the paper. The critical problem highlighted in this paper was misusing the "Digital Security Act(2018)". The author emphasized that frequent cyber attacks on financial institutions are happening because of the misuse of this law. This study used secondary data collection as a research methodology, such as document surveys, content analysis, etc. The author researched from already existing research articles and journals, daily newspapers, and periodicals related to cyber security in Bangladesh. This paper also references reports by the Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) and Bangladesh Institute of Bank Management (BIBM). According to this paper, Bangladeshi banks face up to 630 cyberattacks daily, putting 52% at high risk. The solution that the author came up with is the amidation of Bangladesh's Digital Security Act and upgrading ICT laws. It was also suggested that tackling this type of attack would be easier if the government used international cooperation.

Baqer. M. et al. [13] discussed the concept of the e-police system in Bangladesh. This paper aims to enhance a proper E-police system where people can communi-cate with the police department without hassle. The authors found some drawbacks and shortcomings; simultaneously, they proposed solutions where the government and the authorities can improve the E-police system. This research paper discusses the implementation of the E-police system in the con-text of Bangladesh. The methods used in this paper are a step-by-step approach to software development and technological infrastructure improvements like the estab-lishment of WAN (Wide Area Network) and MAN (Metropolitan Area Networks). Another method is the use of specific technology. This paper mostly used a quantitative dataset involving criminal records, traffic data, yearly crime statistics, and police-people ratio. They also used qualita-tive data, such as citizen information and incident reports.

M. K. Alam [14] analyzed the legal angles of the cybercrime aspects of Bangladesh. They highlighted that Bangladesh, as a developing country, has adopted more technology in their regular life than before, and because of this, cybercrime is also increasing. However, neither the people of this country nor the law enforcement are fully aware of these rising threats to their day-to-day lives. They analyzed case studies, published materials, crime reports, etc., as their primary methodology. The proposed solution for this problem is a multi-faceted response strategy. Which mainly focuses on creating a national cybersecurity policy and developing a computer emergency response team (CERT). They have also suggested strengthening

law enforcement agencies with specialized units dedicated to cybercrimes.

IEEE Security & Privacy Workshops presented VirSec, a new Virtual Reality (VR) testbed which recreates real-world issues in security to learn the usability problems in a controlled yet extremely immersive space [15]. So on this platform, researchers can see how users actually behave under stress and realistic task conditions that are difficult to set up in the lab. Through simulations of cyber-attack reporting and threat management scenarios, VirSec may offer insight into not just where users make mistakes, but how terms are understood under cognitive load, and what bottlenecks are experienced during security-sensitive tasks. Its immersive characteristics can reveal underlying usability problems that might lead to refusal or failure in actual situations. The study shows the utility of using VR as a pre-deployment validation tool for systems with complex configurations and operational procedures in order to minimize cost-intensive redesigns post-deployment. For Bangladeshi cybercrime portals, we believe this approach means that new reporting interfaces could be tested with simulated traffic for user errors and abandonment before going live at scale, increasing user confidence in the system's effectiveness.

Tsakalidis and Vergidis carried out an extensive review of cybercrime community research that focuses on participatory models interested in bi-directional communication between the authorities and society [16]. Trust and continuous engagement in cybercrime reporting, they suggest, can be significantly influenced by reciprocal communication features through which a variety of channels are available to reporters (i.e., live chat support, regular progress status updates over the submitted cases at least between parties involved with reports) as well as interaction models generating system feedback visible to those submitting reports. For the methodological approach they analysed current research methodologies and support platform features which help or interfere with ongoing user participation. For countries like Bangladesh, where confidence in formal institutions may be low, incorporating real-time feedback and interactive tracking of progress into digital portals can provide the user with a greater trust and encourage reporting.

Martins and Correia's multi-vocal literature review is adequate on a variety of levels, in particular regarding integration of expert generated with crowdsourced intelligence on cybercrime threats [17]. Their review exposes significant shortcomings of threat intelligence systems related to the issues raised in Human-Computer Interaction (HCI). They see intuitive categorization schema, good visualizations, and real-time analytic dashboards as tools to make it easier for both technical and non-technical users to interpret the information and make quicker decisions. On the other hand, badly designed intake mechanisms and overcrowded dashboards generate 'noise' that is costly both to data quality and to user efficiency. For the Bangladeshi public crime reporting databases, following these principles would mean to develop backend and frontend systems that can generate hierarchical presentations of categories, interactive visual analytics for the law enforcers and feedback loops that gives the citizenry assurance that their suggestions are being processed in a timely manner ultimately leading to more trustworthy and smarter intelligence cycle.

Kuo and Tang [18] focused on prototype privacy and security systems which are informed by expert usability insights in order to underpin the design of a system that is more lucrative in terms of balancing security needs with user experience. Their work obtained expert feedback across different domains to understand pain points in privacy/security system design (e.g., unclear alerts, complicated authentication and inconsistent messages) which cause the users not comply with the systems. By quickly prototyping and iterative user testing, they even extricated themselves from several police experience skews. The paper stresses the need for including usability professionals early and throughout development in order to avoid expensive deployments with patches. For Bangladesh's cybercrime reporting gateways, such an expert-driven prototyping approach can facilitate the creation of a reporting apparatus that not only is secure and regulatory compliant but also easy to understand and use from an end-user perspective by enforcement officers.

The MDPI Sustainability [19] paper presented the combination of cybersecurity, usability and HCI principles within energy management systems to enhance security, and offered transferable knowledge for other critical information systems . The focus of the framework on reconciling usability and security via adaptive interfaces, real-time feedback, and transparent workflows is very suitable in cybercrimes reporting scenarios. For Bangladesh, embedding such an HCI-informed design framework in its Police Departments might lead to vastly improved security, usability and widespread acceptance without losing on protection rigour.

2.2.2 Crime reporting systems of other countries

Ndubuisi et al. [20] identify a relatively open app for improving the observation of criminals and crime intervention by the police forces through the continuous flow of crowdsourced reports. It is an application, DigiPolice, through which citizens can report any event or act of violation they come across in their day-to-day activities to the police commissioners without the need for the Internet. The main goal is to enhance understanding of situations, available resources, and responses to them using applications based on collective input. The technologies employed by the UK police today, including facial recognition, have raised ethical issues, and their real-time operations in big cities still need to be improved. The work suggests creating a new crowd-sourced reporting application, allowing citizens to report crimes or suspicious activities in real time. It includes real-time reporting from users and supports data collected from various people; this helps the police monitor and act appropriately.

G. Tsakalidis and K. Vergidis [21] address the complexity and scale of the cybercrime threat, which has been an emerging reality for the society and economy as it is a major economic, social and security issue. Further, the authors reveal that inadequate definitional frameworks and classificatory systems are significant challenges that hinder efficient tracking and control of cybercrime occurrences. Employing structured databases from law enforcement agencies such as Europol and FBI and peer-reviewed publications, they develop a dual-tier taxonomical model based on a hybrid schema to categorize and describe cybercrime events based on their significant properties. Based on the findings of the work, it concludes that the suggested approach improves knowledge acquisition, makes revisions and extraction of incidents

more accessible and more efficient, and truly aids in formulating superior policies and event management.

S. W. Smith [22] aim to draw attention to the gap between users' mental models of system security and actual security functionality and the poor security decisions resulting from this misalignment. The research presented in this thesis is based on workshops and interviews, and we argue that the usability security of conflict emerges from overly complex systems, which non-experts do not understand completely outlines a means to bridge the gap between the current state and policy: communication and user-centred security design supported by collaboration between HCI and security experts. The results call for interdisciplinary research into developing such systems that are both usable and secure, and practical studies and prototype development appear to be a better approach to addressing these issues.

E. Sun and N. H. Hassan [23] discuss developing the Smart Cybercrime Incident Reporting System (SCIRS), a web-based application aimed at helping internet users in Indonesia report cybercrime incidents. In addition to reporting, the platform also provides educational content to raise awareness about cybercrime and cybersecurity practices. The primary focus is on increasing cybersecurity awareness among Indonesian internet users, as the country has experienced a significant rise in cybercrime incidents. There is a lack of user-friendly, easily accessible platforms for reporting cybercrime incidents in Indonesia. A web-based platform where users can report cybercrime incidents. It includes live chat support and categorizes reports for individuals and organizations. The platform also provides educational content on protecting devices, social media accounts, and data from cyber-attacks. By simplifying the process, the system aims to encourage victims of cybercrime to report incidents quickly and effectively. Providing real-time support from cybersecurity experts could enhance the platform's value. Leveraging data analytics to detect cybercrime trends and preemptively warn users could improve the system's efficiency.

Weijer et al. [24] address the expanding problem of cybercrime victimization and the lower rates of reporting behaviour among Dutch citizens. The problem discussed in the present work is the difference in the rates of actual reporting to the police, even if victims have reported higher intentions. However, there is an intention-behavior gap in victims due to the lack of trust in the police and dissatisfaction with the previous police's indifferent responses. Results show that victims expressed high reporting intention, whereas only 13% reported their cybercrime experiences to the police. Based on the research done, the study supports the notion that police enhanced collaboration with requisite bodies could serve to enhance reporting rates.

Aairam et al. [25] present a complete Cyber Crime Reporting System implemented as web application for users without much knowledge, especially non-expertise user. The system includes features such as multi-language support, speech-to-text input and intuitive navigation to facilitate various populations and technical proficiencies. It provides safe complaint registration by preserving the confidentiality of data including facility of immediate response to the complainant and faster communication with him. The focus on multi-lingual and oral input interfaces makes this method

particularly appropriate for multilingual literate or illiterate populations. Therefore it provides a scalable, democratic model, and fits to human-centric design aims of cybersecurity reporting.

Breen et al. [26] introduce the first large scale empirical study of the usability and design of cybercrime reporting mechanisms and how this influences potential victim behaviour versus actual reporting taking place. The findings suggest that there is substantial underreporting associated with unclear processes, disconnected systems, and interfaces that lack adequate support or response. Victims often describe confusion related to variation in nomenclature and lack of direct follow-up protocols, which lead to non-completion of reports. The authors posit that synchronizing user interfaces to provide centralized reporting portals with clear case management, progress tracking, and simple language instructions will help overcome these challenges. This study highlights the necessity of incorporating user-centered design and transparency of process into their system to build trust and higher reporting rates to aid in law enforcement's overall crime-abatement strategies.

2.2.3 Cybercrime in the financial sector (India)

Y. M. Jadhav [27] have the critical goal of analyzing the efficiency and usability of India's National Cyber Crime Reporting Portal in the context of the fight against financial cybercrimes. This paper identifies and explains the current status of the portal for countering financial cybercrimes and delivers suggestions on how it can be improved. The case studies showed that, on some occasions, the portal was instrumental in investigations. Intensifying cooperation with the police, private companies, and civil society organizations is necessary to achieve faster restoration of justice in cybercrime. It is adding more sophisticated technology aspects of chatbots that are considered to be based on Artificial Intellect and include real-time assistance for clients who would have experienced cybercrimes.

According to Babar et al. [28], in the context of India, there are several issues with the crime management system. Because of these management issues, many people do not feel the safety or urgency to report a crime when that occurs. Due to this lack of reporting practices, crimes are increasing in India. They have used the Modified Waterfall methodology to develop the website. This paper does have some research gaps, such as not considering how the system database will flow with law enforcement so that the crime investigation becomes seamless. The system also does not mention any particular data privacy and security issues, which will be a significant issue in this case. As crime reporting is happening online, the report can also be fake, so the procedures for differentiating between real and fake crime must be more apparent.

Puchalski et al. [29] integrate state-of-the-art AI techniques for cyber-attacks detection along with user-friendly, explainable interfaces aimed at law enforcement and cybersecurity analysts in their work ([29]). We focus on human-computer interaction principles, such as transparency, user control, and interpretability to show the challenges of building trust with AI systems that manage sensitive operations. By

systematically integrating advanced backend analysis with comfortable frontend design, their work fills up the ragged edge between leading AI capabilities and actual usage experience in cyber operations. Its methodology demonstrates the importance of HCI perspectives for realising successful rollout of technologies for automated detection and reporting cybercrime.

2.2.4 Awareness of cybercrime and protection

M. N. Rita and F. B. Shava [30] present the development of a website that utilizes a chatbot interface to educate the population of Namibia on online child sexual exploitation. The website offers the opportunity to report abuse incidents that occurred online and helps increase awareness of online risks. The developed concept for the interactive website incorporated a chatbot. It was piloted, showing that children would report an incident or turn to the website for information about online safety. Students are victims of scammers and experience obscene messages because they have free access to technological gadgets. Creating a website with a dialogue area and a chatbot is intended to receive reports from children and open the material about safety on the internet. The website allows children to report other children for abuse noticed online, and they can do this anonymously, meaning that they will not be restricted by fear of anyone knowing they reported someone they know for abuse. The participants appreciated the need to be taught how to stay safe online. From the results of the remote usability testing, it can be seen that respondents found the website and the chatbot easy to use and helpful in raising awareness. Including a person's law enforcement along with psychologists and social workers to provide more extensive help on the Website. Incorporation of online safety as a subject in the curriculum to reach most students online.

Khairy et al. [31] investigate reporting systems, user awareness of privacy settings, and experience of cyberbullying among Facebook users. The study surveyed 273 Facebook users and found that users don't know how to effectively utilize privacy settings features and reporting systems. A significant majority of respondents (83.1%) reported using privacy settings on their accounts, indicating high awareness about such features. However, 7.1% of respondents did not know what privacy settings were, suggesting some gaps in understanding among users. In this research, the author found several problems related to user awareness of privacy, reporting systems, and cyberbullying on Facebook. Those problems need to be more understood: lack of knowledge of privacy settings, statistical correlations and relationships, users needing to prioritize their privacy on social media, and cyberbullying on social media. This research suggests that simplifying the reporting system to be more user-friendly can be more productive. Enhancing user education and awareness campaigns is an efficient approach. They are establishing a support system for users who have experienced cyberbullying. Also, the author mentioned other approaches, such as the incorporation of feedback mechanisms, the focus on regular updates, and collaboration with educational institutions.

Murtezaj [32] to build Public Security User Interfaces, or PSUIs beyond plain cybercrime reporting systems through the user interface aiming at fostering a pro-active safe and secure use of ICT . The paper suggests that raising cybersecurity aware-

ness should involve integrating security prompts, visual (aural) feedback and nudges into generic experience of a user interacting with the digital environment. Employing iterative user-centered design and qualitative inquiry, Murtezaj illustrates how intuitive design can make it easier for practitioners to minimize errors as well as promote safer practices without overburdening users. Contrary to such systems only designed for incident logging, this work focuses on the overall participation of security awareness and motivation, which is highly applicable to those who have very low cyber-security literacy. The planned UI models will include context aware warnings, progress indication, and educational suggestions to enable users for self correction and due diligence. This work makes a contribution to HCI by recasting security as an ongoing interactive practice, and pointing out that the development of cybersecurity culture relies fundamentally on open design principles and empowered users.

Jacobs [33] studies the psychological and cognitive toward understanding users' behavior in cybercrime reporting, highlighting trust, transparency and cognitive load as key factors of user interface design . Through combining surveys, interviews and usability testing approaches in mixed methods research this study finds that in the face of complex and opaque systems with minimal feedback, a significant portion either drop off from using or choose not to report. If real-time status updates, estimated durations and clear confirmation messages were offered on interfaces, users were more inclined to report by having trust in the reporting process. In contrast, high cognitive load and disoriented navigation were known causes for drop-outs. The results indicate that the involvement can be increased by decreasing information load with an incremental disclosure and simplifying reporting workflow. Significantly, Jacobs also stresses that building trust through transparent communication is just as important as the strength of the algorithm itself in keeping users involved. These findings contribute to HCI design by demonstrating that psychological comfort needs to be prioritised as well as security when designing for improved cyber crime reporting effectiveness.

Elsevier's making security awareness and training broadly available, cognitive considerations in cybersecurity education [34] , takes a planning approach to cognitively accessible cybersecurity training: This is training that is designed with the understanding of how people learn new material . The authors identify the cognitive challenges users encounter in complex security scenarios and promote training strategies that provide clear language, scaffold learning into bite-sized tasks, and are delivered in interactive, entertaining formats of different levels. Access here includes not just cultural and linguistic accessibility, but inclusive design for diverse publics. They recommend using easy language, presenting examples from context during learning and providing adaptive feedback to the learners. These principles are especially appropriate when applied to cybercrime reporting tools in Bangladesh where end-users can be of different literacy level, knowledge on digital security. By embedding easily usable training material into a reporting portal, people can become better equipped to recognize and report incidents and develop more general awareness of cybersecurity.

2.2.5 Cybercrime Management: Law and Policy Gaps

S. G. Correia [35] assess the advantages and drawbacks of utilizing AF data, especially in law enforcement research and another user study, and highlight the importance of improving data quality across several dimensions: an updated list of characteristics, which includes relevance, accuracy, reliability of the information, coherence in thought, and ease of access. Cybercrime and fraud are some of the most under-reported cases, compromising the representativeness of AF data. It is reported that AF receives only the tip of the iceberg; computer misuse and fraud, respectively, are reported to AF at only 2% and 8%. Various forces record data using different methods, creating gaps that make it hard to analyze or compare data properly. This study primarily discussed fraud and computer misuse cases during the COVID-19 outbreak, with 11,934 reports collected between February and June 2020. The study reaffirmed prior research, suggesting that cybercrime and fraud are hugely under-reported and substantially more than what is noted in the British Crime Survey or, in fact, the official crime statistics. It is therefore recommended that future research seek to improve the Policing 'Protect' model to support the victims, particularly those who are vulnerable to repeated victimization. However, further fulfilment is required on how data accumulation and documentation processes are standardized across police forces to enhance the degree of correspondence and logical flow.

Harjinder Singh et al. [36] highlighted all the cyber attacks during the COVID-19 pandemic. People faced many cyber issues during COVID-19, mainly as individuals worked from home and software vendors. The goal was to improve cyber security in a post-pandemic world. During the COVID-19 pandemic, several types of cyber attacks increased significantly, including phishing attacks, ransomware, malware, extortion attacks, spam and malicious URLs, fraudulent online shops, etc. A systematic approach method was employed in this research to analyze cyber-attack-related problems in the COVID-19 pandemic. The critical methodologies are timeline creation, attack categorization, data collection, and case study approach. The key characteristics of the datasets are temporal data, geographical scope, source of information, and incident reports. The author also provides some recommendations for improving the situation in a post-pandemic world. For example, strengthening cyber security, awareness of cyberattack patterns, collaboration and information sharing, developing comprehensive cyber security strategies, education and training. The paper's conclusion emphasizes the impact of the COVID-19 pandemic on the landscape of cyber security. This paper highlights the significant increase in cyberattacks and the vulnerabilities of various sectors.

Nouh et al. [37] propose a problem-based approach to investigate all the difficulties experienced by police officers when solving cybercrime cases arising from the deficits of technical knowledge and lack of efficiency in available technologies. Interviews with key informants also showed the deficiency of improved training and the call for user-oriented instruments for psychological cybercrime investigators. Current systems need to improve in usability, which hampered intelligence. To address these gaps, the authors suggest improving communication and tool design. They also point to additional research in determining the exact process and tools for investigators to function optimally. The study also stresses the need for more research into

training requirements and enhanced information exchange structures.

Leuprecht et al. [38] aim to discuss the critical aspect of the UAE's general population's inadequate level of cybersecurity awareness, compared to the USA, as it is preconditioned by its cultural, educational, and legal backgrounds. The present study aims to compare the level of awareness of cybersecurity threats of STEM respondents from the USA and UAE through a causal-comparative research design and self-administered surveys completed by 157 USA and 165 UAE participants. It was established that UAE participants recognized a significantly lower extent of Cybersecurity threats. Based on these threats, the authors recommend the following strategies: capacity building, legal changes and creating a cybersecurity culture. The findings underscore the importance of context-specific approaches in the UAE about human aspects that affect cybersecurity disposition. More studies are recommended to enhance subsequent survey tools and develop accurate regional cybersecurity campaigns.

M. Bidgoli and J. Grossklags [39] shed light on the critical problem of underreporting in cybercrime incidents and point out the significant issues and possible areas for improving the reporting process. The authors state that the number of cybercrimes remains unknown because many cybercrimes are never reported for various reasons: victims may be unsure as to whether they have been the victim of a cybercrime; they may not know how to report the crime, and users still lack confidence in reporting such crimes. The paper outlines four main challenges that hinder effective cybercrime reporting: describing what is meant by cybercrime victimization, raising awareness on reporting a case, encouraging reporting of cases, and guiding users when reporting cases. These authors also call for more research on the users' behaviours and processes of reporting cybercrime and how the current reporting solutions can be re-designed. Therefore, the paper concludes by advocating for engagement with researchers, police departments, and cybercrime organizations to address the weakness in the cybercrime reporting system, with an overall goal of increasing the effectiveness of combating cybercrime and increasing public awareness of the problem to instil dread in society.

Sakpere et al. [40] present the CryHelp App that can be adopted for safe crime reporting in contexts with limited resources. It applies to underreporting because of concerns about privacy and issues with the user interface. The app uses a user-centred design process; users can file reports with little text input, and it comes with an emergency button. In terms of usability, testing revealed issues with the interface and navigation, although an overall rating was achieved through testing with university students of 77.06%. This research indicates that more user training efforts and interface enhancements, especially in limited-technology environments, remain essential to increasing crime reporting.

Bidgoli et al. [41] identified that many cybercrimes go unreported and cause problems for law enforcement in the USA. According to the authors, this happens because of ineffective reporting mechanisms. Because of this, misdirected unrelated reports also get field. They have provided data about PayPal, and they receive about 10,000 misdirected emails per month, which their automated system cannot handle.

The authors developed a design that can help customer-facing cybercrime reporting interface. This could reduce the burden on any personnel handling the report by himself. The paper used a usability testing dataset for research. They took 523 people from Amazon Mechanical Turk (AMT) to participate in scenario-based testing. They evaluate the design based on this usability and effectiveness testing. Using statistical models, the authors examined the connection between users' impressions and their propensity to report cybercrime. That study received positive feedback. According to the study, the suggested interface is user-friendly, potentially resulting in increased cybercrime reporting compared to before. The results indicate that self-efficacy, awareness of cybercrime severity, and past victimization positively impact user reporting behaviour.

Springer-Verlag et al. [42] presented an in-depth inquiry into why and how security and usability should be co-designed to prevent contradictory needs from undermining trustworthiness and potential effectiveness . The paper disseminates the issues where tight security controls impose usability burden by users and conversely, simple interfaces weaken security claims. The conclusion of the authors based on in-depth study of system specifications and real-world examples, for an optimal approach, features agile security mechanisms specially designed to be tuned based on user context and risk levels. This has huge implications for cyber crime reporting portals: adaptive security measures that prioritize necessary protections without becoming too complex or annoying are key. In developing contexts, such as Bangladesh, it is evident from our study that designing scalable-yet-usable reporting systems calls for careful consideration of not only technological boundaries but also interface design and user training to foster resilient and trustworthy platforms.

2.3 Research Gap

Previous research has studied multiple cybercrime reporting systems such as user-friendly applications and automated reporting interfaces yet most of these solutions struggle with usability problems and accessibility barriers and do not encourage sufficient reporting. Our research project will develop an optimized cybercrime reporting structure specifically addressed for the needs of Bangladesh to overcome identified shortcomings. The model we propose implements various improvements over existing models through its user-friendly interface combined with multi-layer security authentication and reports processes that require less user interaction. A detailed evaluation with numerous user groups will be performed through usability testing to confirm system effectiveness for authentic practice. The research findings will advance the development of an inclusive cybercrime reporting system that national governments can implement across the country.

Chapter 3

Methodology

This chapter describes the comprehensive approaches used by our research to evaluate the usability of the existing cyber crime reporting systems. Since these platforms carry out such vital role in digital safety, we applied three key methodological experiments which are: heuristic evaluation, user testing, and semi structured interviews. Direct user experiences were captured through user testing to quantify practical interaction difficulty, task completion rate, areas that frustrated them. And finally to understand the organizational perspective, we conducted semi structured interviews with officials and looked into the challenges that they face in ensuring and enhancing the effectiveness of these platforms. These three methods together made it possible to carry out a comprehensive assessment, with both expert observations and real user insights fed into the research. Data collection methods and analysis procedures are described in detail below and how participants were recruited. Our workflow is shown in Figure 3.1.

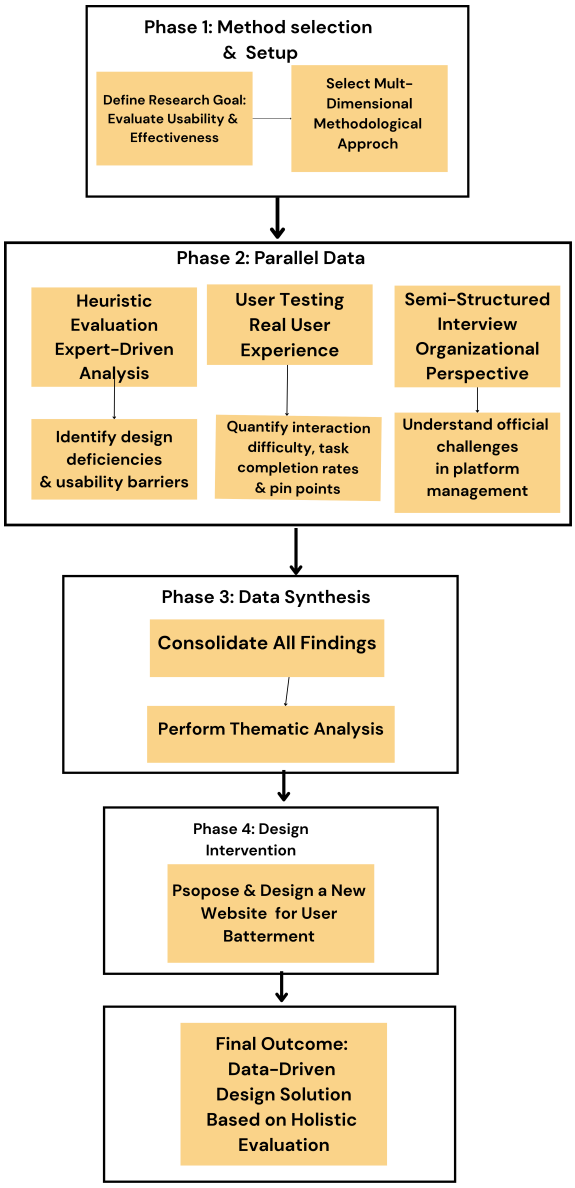

Figure 3.1: Work Flow

3.1 Participants

This study incorporates three groups of participants to ensure a holistic understanding of the usability challenges in cybercrime reporting systems. The participants were approached within the range of the researchers' social network (friends, Family, and colleagues). Their involvement was voluntary, and they received no recompense or incentives. The time and energy they gave to this study were entirely from goodwill.

3.1.1 Heuristic Evaluation

The heuristic evaluation utilized five members of our thesis group as expert evaluators to perform the analysis. The expert evaluators used Nielsen's Usability Heuristics [7] standard to evaluate the usability elements in the websites from the Crim-

inal Investigation Department (CID) and Bangladesh Telecommunication Regulatory Commission (BTRC) and Digital Security Agency (DSA) as well as the Online GD application. The analysis attempted to determine usability failures through set benchmark criteria as well as through professional intuition.

3.1.2 User Testing

A systematic user study was performed on the mentioned government websites (CID, BTRC, DSA and online GD app). Here 40 participants took part, aged between 22 and 37. The base for the recruitment were to specifically focus on a younger to mid aged audience who are regular users of these technological platforms. This sampling method resulted in an adequate representation of the study population and possible user groups, increasing representativeness of our findings. Findings from user testing allowed us to systematically find major usability problems, from difficulty navigating an interface to preventing or hindering task completion. Through empirical support of usability problems, we have established a strong ground for identifying and targeting improvement for HCI principles overseas the rehabilitation of government reporting websites.

3.1.3 Interviews

We conducted semi-structured interviews with five officials: an official of the National Security Intelligence (NSI), a Sub-Inspector of the Dhaka Metropolitan Police (DMP), two representatives of the Security Solution Implementation Department of the Bangladesh Financial Intelligence Unit (BFIU), and one of the officials from Dhaka Metropolitan Police (DMP) Cybercrime Unit. The interviews focused on revealing issues that these organizations experienced throughout system implementation and maintenance. The interview design provided deep understanding about technical challenges alongside operational constraints and user experience problems.

3.2 Data Collection Methods

Qualitative insights were obtained using a combination of diversified data collection methods.

3.2.1 Heuristic Evaluation Process

The heuristic evaluation followed a structured process wherein each evaluator reviewed the platforms individually against 10 usability heuristics, such as:

1. Visibility of System Status.
2. Match Between System and Real World.
3. User Control and Freedom.
4. Consistency and Standards.
5. Error Prevention.

6. Recognition Rather Than Recall.
7. Flexibility and Efficiency of Use.
8. Aesthetic and Minimalist Design.
9. Help Users Recognize, Diagnose, and Recover from Errors.
10. Help and Documentation.

All the usability concerns were rated by the levels of the severity: minor, moderate, severe, or critical. Combined findings were used to provide guidance to system redesign with essential usability issues being identified that became necessary during redesign order.

3.2.2 User Testing Protocol

The participants were then required to perform three pre-planned operations exercises, which included complaint registration and help navigation as well as evidence upload procedure. They noted the following:

1. Task Completion Rate: The test established whether the users were able to complete whatever they were given to do.
2. Time on Task: User completion time is one of the measurable features. employed to work on certain tasks.
3. Errors and Frustrations: Users complained of problems and incidents where they ceased their operations.
4. User Response: Users provided direct verbal feedback on usability and design aspects.

The information gathered in the course of testing included the use of the think-aloud technique, enabling the subjects to state their mind, and standardized tests ensured the objective result of the analysis [43]. The technique enabled researchers to record both user behaviours along with their mental processes while they formed their expectations.

3.2.3 Interview Guidelines

The conducted interviews focused on operational challenge analysis and strategic information regarding cybercrime reporting systems. Both of these sessions were about 30-60 minutes long and discussed the following topics:

1. Technical Challenges: The current systems have issues with maintenance and scale-up tasks.
2. User Feedback Integration: The existing user feedback integration process and activation of organizational responses to received input needs to be tested.
3. Operational Gaps: Proposals exist toward improving the operational efficiency and user-friendly quality of the systems.

To probe recurring themes and insights, we analyzed transcripts from interviews we conducted with permission along with tape recorder recordings.

3.3 Ethical Considerations

The study maintained extensive enforcement of ethical principles from start to finish. All participants received information about study goals followed by obtaining consent before starting the experiments. All personal data received secure anonymization along with dedicated room storage for exclusive research usage. Documentation seeking and securing ethical authorization was achieved through appropriate institutional review boards.

Chapter 4

Usability Testing of the Government Cybercrime Reporting System

To gain more insights into the usability issues with existing government cybercrime reporting websites, usability testing was conducted on the Criminal Investigation Department (CID), Bangladesh Telecommunication Regulatory Commission (BTRC), and the Digital Security Agency (DSA), as well as one Android mobile app, called 'Online GD' in order to evaluate the usability, accessibility and overall UX [1] [2] [3] [4]. User testing is a core HCI practice, which entails observing and interacting with real users as they undertake specified tasks to identify practical problems and experiential bottlenecks that heuristic evaluations are unlikely to detect. This method is used in the study to assess the quality of support these digital platforms provide for their users. The aim of introducing this method in this work is to evaluate how well these digital platforms assist their intended users and identify areas where usability could negatively impact efficiency, confidence, and overall satisfaction. Here, an overview of participant details and methodology is provided, followed by reflections on issues unearthed by task-based tests and "think-aloud" activities.

4.1 User Testing

In the field of Human-Computer Interaction (HCI), user testing is one of the most basic methodologies to facilitate systematic user testing of the functionalities of digital interfaces and how they are accessible to end-users. Contemporary scholarship acknowledges that analyses that focus solely on task-related issues fall short of capturing the multifaceted determinants of user success or failure within web-based environments. A growing need within human-computer interaction is to explore user-experience explorations thoroughly.[43] Authentic users complete product-oriented activities, e.g., browsing a website, interaction with an application, under controlled (observational) study findings on usability defects, operational deficiencies, and opportunities for improvement [44], [45]. The challenge of user testing is to create a system that caters to users in every way possible, allowing all types of users to use it easily, and addressing their needs or expectations. The problem of user testing is related to creating a product design that meets consumer demand while also addressing specific expectations or requirements. Deliberately introducing compound

phenomena during a testing session and responding to them accordingly can help designers create intelligent, efficient, and engaging interfaces for particular honeycombsegments of the population [46]. In Markville's honeycomb, Human-Computer Interaction is defined by seven key qualities (Figure 4.1) of User Experience: findability, accessibility, usability, usefulness, credibility, desirability, and value [47]. A quick definition of these terms:

- **Findability:** How do users actually find what they are seeking on websites?
- **Accessibility:** The system needs to eliminate physical restrictions that prevent users from accessing it, as well as accommodate disabled users.
- **Usability:** Are users satisfied while using this product?
- **Usefulness:** Are users finding the product useful in their daily lives?
- **Credibility:** This section tests if the product is trustworthy for users.
- **Desirability:** Are users showing positive emotions toward this product?
- **Value:** The product serves what purpose toward the organization that stands behind its creation?

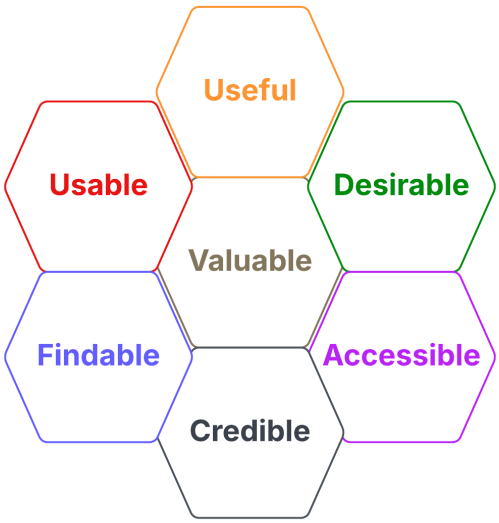

Figure 4.1: Morville's Honeycomb Model

4.2 Why User Testing for this Research?

Within the context of this study, user testing is essential for analyzing the usability of crime-related government websites and assessing user satisfaction, with the aim of recommending improvements. The role played by public-service websites remains crucial, so their usability should be optimized to enhance accessibility and effectiveness.

The specific purposes are:

1. Finding out what drives users away from using the systems.
2. Attaining user input on elements inside the system that have to be enhanced.
3. Developing suggestions for operations that should be intended to optimize the quality of the user interface.

The heterogeneity of participant backgrounds provided a valuable source of insights, offering both technical and non-technical perspectives. By accommodating users with different levels of expertise, the study of the platform's performance contributed to the evaluation of usability issues common to all users. This User testing allows deeper insights into how a product works. The real-time user actually perceives a system, which allows the priorities and aspirations for improvement to be identified simultaneously. According to research by Maguire and Isher [45], expert knowledge can help guarantee the success of information retrieval. According to their findings, the collaboration of the experts not only makes the process of retrieving the results much easier but also enhances the quality of the results. Further investigation may yield additional insights on how to facilitate greater efficiencies in systems [45].

4.3 Participants

Forty(40) participants participated in a moderated user study to assess the usability and accessibility of three government websites, including CID (Criminal Investigation Department), BTRC (Bangladesh Telecommunication Regulatory Commission), and DSA (Digital Security Agency), as well as one mobile application, Online GD. Recruitment involved a multiprofessional and multigrade workforce to ensure diversity in views and experiences.
The user testing sample size consisted of sixteen(16) females and twenty-four (24) males. The age group was selected to be between 21 and 37 years old. The largest group among this was university students (aged 21–27), who accounted for 21 participants. A similar, but much smaller, group of mid-career professionals includes doctors, IT workers, nurses, bank or university lecturers, between the ages of late 20s to mid-30s(Figure 4.2).
Concerning occupation, a majority of participants were university students (n = 21; 52.5% of the data sample). These students studied in various disciplines, including Computer Science and Engineering, Law, Business Studies, and Public Health, at renowned universities in Dhaka, such as BRAC University, North South University, United International University, and Independent University, Bangladesh. The second-largest category consisted of seven(7) doctors and four(4) nurses, followed by three(3) IT technicians, three(3) bankers, one (1) lecturer, and one(1) trainee engineer(Figure 4.1). This variety enabled the research to incorporate the views of both technical and non-technical users on digital government platforms (Figure 4.3).

About personal exposure from online crime, eight respondents reported that they themselves had been the victim of an experience with online fraud and harassment or cyber threats. Of those, five people attempted to access the CID site but failed; they then reported their problems in person through regular police stations. While

the study was underway, three players attempted to report valid complaints to the system. Participants who were not influenced to report due to a personal experience instead indicated how they would respond in mock scenarios, inspired by typical cybercrime reporting encounters, leading to valuable usability data where they had not previously endured a cybercrime incident.
Online usage was high amongst the participants, and the majority were daily users of digital services. They had a range of technological experience, although some had high levels of technical knowledge, having studied computer science or worked as IT experts. Others worked in healthcare or banking and may find digital navigation, access, and confidence with reporting systems more challenging (Table 4.1).

This variety of mixed users helped researchers to identify usability problems that apply to both high- and low-level users. The presence of respondents with previous exposure to cybercrimes, as well as newcomers to these systems, allowed group members to identify design failures, accessibility challenges, and trust issues on the analyzed platforms.

Figure 4.2: Participants

Table 4.1: Demographic Details of Participants

Serial No.	Gender	Age	Profession	University/ Place of Work	Internet Use Frequency	Knowledge About Cybercrime
1	Female	22	Student (Major: Computer Science & Engineering)	North South University	Daily	In-depth knowledge. Study Field: Cybersecurity.
2	Male	24	Student (Major: Computer Science & Engineering)	United International University	Daily	Familiar
3	Male	24	Student (Major: Business Studies)	Independent University, Bangladesh	Almost Everyday	In-depth knowledge. Faced this and went through the legal procedure.

Serial No.	Gender	Age	Profession	University/ Place of Work	Internet Use Frequency	Knowledge About Cybercrime
4	Female	21	Student (Major: Bachelor of Laws)	North South University	Daily	Not very familiar. Knows about online bullying and fake ID
5	Female	24	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
6	Male	23	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
7	Male	24	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
8	Female	23	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
9	Female	23	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
10	Male	23	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
11	Female	24	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge
12	Female	27	Student (Master's in Public Health)	North South University	Daily	In-depth knowledge
13	Male	24	Student (Major: Computer Science & Engineering)	Independent University, Bangladesh	Daily	In-depth knowledge
14	Male	23	Student (Major: Bachelor of Laws)	BRAC University	Daily	Familiar
15	Male	24	Student (Major: Bachelor of Laws)	United International University	Daily	Familiar
16	Female	24	Student (Major: Computer Science & Engineering)	Independent University, Bangladesh	Daily	In-depth knowledge. Faced this and went through the legal procedure.
17	Female	24	Student (Major: Business Studies)	United International University	Daily	In-depth knowledge. Faced this and went through the legal procedure.
18	Male	22	Student (Major: Business Studies)	United International University	Daily	In-depth knowledge. Study Field: Cybersecurity.
19	Male	24	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge. Study Field: Cybersecurity.
20	Male	24	Student (Major: Computer Science & Engineering)	BRAC University	Daily	In-depth knowledge. Study Field: Cybersecurity.
21	Female	33	Doctor	Shaheed Suhrawardy Medical College & Hospital	Frequently	Familiar
22	Female	31	Doctor	Shaheed Suhrawardy Medical College & Hospital	Daily	In-depth knowledge. Faced this and went through the legal procedure.
23	Male	31	Doctor	Shaheed Suhrawardy Medical College & Hospital	Daily	Knows about social media fake accounts and harassment only
24	Male	35	Doctor	Shaheed Suhrawardy Medical College & Hospital	Daily	Familiar

Serial No.	Gender	Age	Profession	University/ Place of Work	Internet Use Frequency	Knowledge About Cybercrime
25	Male	29	Doctor	Shaheed Suhrawardy Medical College & Hospital	Frequently	Familiar
26	Male	32	IT Technician	Advance Attire Ltd.	Daily	In-depth knowledge. Faced this and went through the legal procedure.
27	Male	36	IT Technician	Advance Attire Ltd.	Daily	In-depth knowledge. Study Field: Cybersecurity.
28	Male	30	IT Technician	Advance Attire Ltd.	Daily	In-depth knowledge
29	Female	28	Nurse	National Institute of CardioVascular Diseases (NICVD)	Daily	In-depth knowledge. Faced this and went through the legal procedure.
30	Female	28	Nurse	National Institute of CardioVascular Diseases (NICVD)	Almost Everyday	Very little knowledge
31	Female	27	Nurse	National Institute of CardioVascular Diseases (NICVD)	Daily	Familiar
32	Male	28	Nurse	National Institute of CardioVascular Diseases (NICVD)	Daily	In-depth knowledge. Faced this and went through the legal procedure.
33	Male	33	Doctor	National Institute of CardioVascular Diseases (NICVD)	Daily	In-depth knowledge. Faced this and went through the legal procedure.
34	Male	37	Doctor	National Institute of CardioVascular Diseases (NICVD)	Almost Everyday	Familiar
35	Female	29	Management Trainee	The Premier Bank	Daily	Familiar
36	Female	36	Banker	The Premier Bank	Daily	In-depth knowledge. Especially about financial online fraud
37	Male	36	Banker	IFIC Bank PLC	Daily	In-depth Knowledge
38	Male	30	Lecturer	United International University	Daily	Familiar
39	Male	31	Trainee Engineer	PRAN RFL Group	Daily	In-depth knowledge
40	Male	27	Student (Master's in Public Health)	North South University	Daily	Familiar

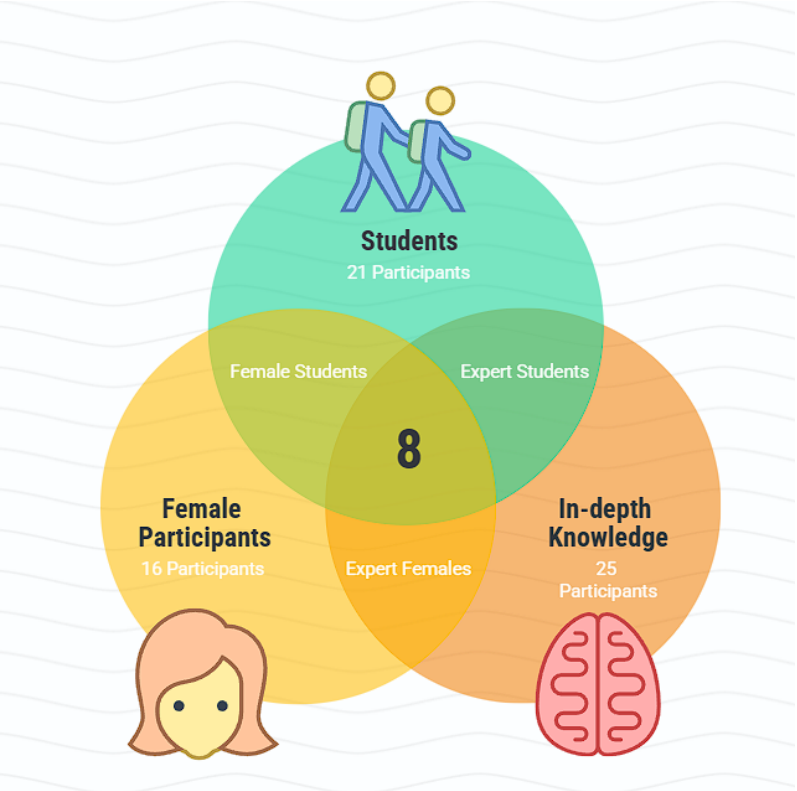

Figure 4.3: Cybercrime Knowledge Demography

4.4 Procedure

In this study, a moderated user testing method was employed to assess the usability and accessibility of three public websites (CID, BTRC, DSA) and one mobile application (Online GD). The testing workflow consists of two scenarios. In one condition, participants were introduced to the websites and mobile applications and then left to browse them freely on their own. In the second condition, participants were invited to complete specific user tasks (e.g., register for an account, file a complaint, find key resources, or upload accompanying documents). In those sessions, the user was invited to voice their thoughts during the interaction using the "think-aloud" protocol, thus allowing for discussion of cognitive processing, frustration, and expectations. Throughout the time, researchers had looked for participants' attitudes as reflected in their facial expressions, hesitation, and body language, which provided them with indicators of potential usability issues that participants were not directly verbalizing.

During task completion, time-on-task was recorded to measure the efficiency of task execution. Upon completing the tasks, all participants participated in a question answer session lasting approximately 15 minutes. These examined the participants' reactions to their experiences with the platforms. Real users with complaints due to prior cybercrimes, as well as users trained to simulate complaints, were included, ensuring that the findings captured a broader range of issues, from those surrounding first-use usability barriers to failures of the system in real-world cases. The data were analysed using thematic data analysis. This analytical approach enabled the research to identify mechanical hurdles, including navigation and safety issues.

Moreover, there are emotional ones as well, such as distrust, frustration, and a lack of confidence in the digital systems for reporting. Finally, the results were analyzed at a higher level, categorized by problem, and contextualized in terms of usability heuristics and user experience principles, allowing the findings to be applied to both design refinement and policy implications.

The principle we use for our user testing:

1. **Task-based evaluation:** Here, users completed some tasks of the CID, BTRC, and DSA websites along with the Online GD mobile apps. The tasks were:
    - Registering or logging into the systems.
    - Looking for forms to submit complaints.
    - Navigation through the websites and app.
    - Looking for valuable numbers on the websites.
    - Submitting proof or documents to the websites, and so on.
2. **Thinking-aloud:** Users were completing each task and communicating with the moderator about what they are thinking about those features and tasks.
3. **Question Answer Session:** This part was about asking questions about what they think should be modified or include in the websites to make it better for them to use and shift to online reporting systems instead of in person reporting.

4.5 Findings

The qualitative and quantitative information obtained from participants was systematically examined, focusing on common patterns, challenges, and respondent perceptions for each of the selected platforms. In this subsection, we present the detailed results for the various compared systems: CID, DSA, BTRC, and the Online GD mobile application. Results are classified by platform to expose ease of use strengths and weaknesses, as well as cross-cutting concerns stemming from accessibility, trust, and system feedback. This allows the analysis both in terms of how participants engaged with the system at the time of use as well as connecting these interactions to broader human-computer interaction (HCI) dimensions to gain insight into how issues of design and function influence engagement with government digital services.

4.5.1 CID

Users uniformly found the CID website to be unusable and non-intuitive for task-oriented reporting requirements. Almost all of the users (38 people) who visited the CID homepage found themselves disoriented due to a mismatched layout and a distracting information architecture. Key features for a reporting system, such as filing a cybercrime complaint, were not immediately apparent where they were expected to be. Twenty-nine(29) users were initially confused about where to find

the complaint form. After finding the "Complaint" link, it led them to an external service called GRS, creating confusion and a lack of trust. Navigational difficulties such as unclear menus, inconsistent nomenclature (structural barriers), and a "back" button malfunction that was unable to return participants to the homepage (behavioural barrier), created several unnecessary dead-ends in relatively straightforward tasks. One user among those who had already faced cybercrime and tried to use this Website quoted "I was already panicking because of my issue, and this website was playing games with me, I have never been more disappointed like that before". In addition, 17 participants attempted to use the FAQ feature for guidance. However, they faced broken and absent support mechanisms, including FAQ pages that were blank and unhelpful, help features that did not function properly, and telephone hotlines that were often busy and could not be connected in some cases. As one user mentioned, "If I give any wrong information or face any difficult situation, I can not get help or resources within this site." Thirteen users mentioned that language support was inconsistent; for example, if the whole Website could be in Bangla as well, it would help them. Thirty-one users found the drop-down boxes very confusing, as every feature had another drop-down feature, which frustrated them. One said, "As this website is also an official site for the Bangladesh CID, they are giving more information about them and less information about how we are actually supposed to use this for reporting." Also, English switches would often display both languages simultaneously, which confused many users and increased error probability as well. All eight participants who faced real cybercrime and attempted to use this Website actually shared that there was no secure or traceable method to submit a complaint using the Website (no confirmation codes, no tracking IDs). After becoming frustrated, they had to report in person and faced many hassles. This lack of feedback and verification damages the credibility of the online channel, contributing to a lower perceived value. (Table 4.2) (Figure 4.4)

Table 4.2: CID Website Usability Issues Mapped to HCI Principles

HCI Usability Principle (Nielsen's Heuristics)	**How the CID Website Failed to Follow HCI Principles**	**No. of Participants Mentioning**
Visibility of System Status	No confirmation or tracking ID is provided after submitting complaints, leaving users unsure if their submission was successful.	40
Match Between System and Real World	Complaint redirection to GRS confused users, as the terminology and pathways did not align with user expectations.	38
User Control and Freedom	The back button often failed to return users to the homepage, causing them to be trapped in loops.	38
Consistency and Standards	Inconsistent language toggle (Bangla/English overlap); important links behave differently across pages.	13
Error Prevention	Critical buttons led to irrelevant pages or broken links, increasing the risk of errors in filing.	40
Help and Documentation	The FAQ page was empty/unhelpful; chat/help lines were non-functional or busy.	17
Flexibility and Efficiency of Use	No quick-access options are available for frequent users; repetitive manual steps are required.	8
Aesthetic and Minimalist Design	The homepage is cluttered with too much text/links, making it difficult to identify key actions.	40
Recognition Rather Than Recall	Users had to guess where the complaint form was located due to poor labeling of essential features.	29
Error Recovery and Feedback	No clear error messages or guidance when links failed or forms redirected incorrectly.	17

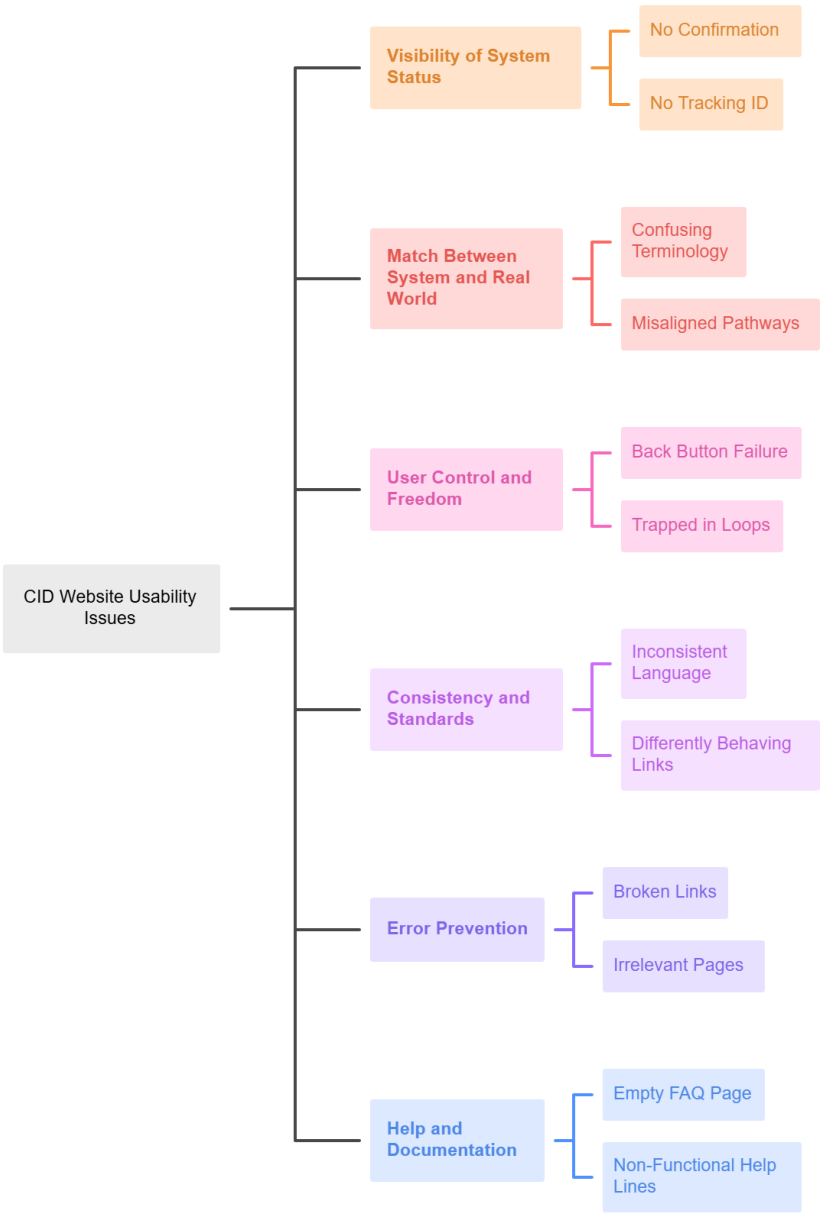

Figure 4.4: CID Website Usability Issues

4.5.2 DSA (Digital Security Agency)

The DSA website elicited concerns about trust, findability, and security. Users told us that this Website only provides information on Bangladeshi cybercrime-related safety, including necessary details. All participants were unable to find a complaint form online, only discovering contact numbers and general information on cybercrimes, as well as departmental information related to that. This Website functioned more like a search engine than an online reporting site. Seven(7) users attempted to call the helpline number, but two(2) of them were unable to get connected, and for three(3) users, the waiting time was so lengthy that they hung up. Two(2) people were able to get connected, but they were asked to visit the nearby police station. When trying to use the chatbot or interactives, it did not work as expected, and

sometimes the page would not load or display an error message. A good thing about this Website was that six(6) users, all of whom were computer science background students, noticed that they had an accessibility button. This button helps visually impaired people. The features included monochrome, inverted colors, a large cursor, highlighted links, show headings, a reading guide, reset, download screen reader, and keyboard shortcuts. Except for the keyboard shortcut, all the other accessibility buttons work. They mentioned, "This website really gave a thought about people with visual impairment but then again no one can make a complaint here if needed so there's that downside".
Additionally, two(2) users' browsers who were using a MacBook at that time warned that the Website was "dangerous," a significant credibility issue that undermined confidence in the service. The organization of the site and its navigation functions were often characterized as disordered, confusing, and monotonous, with many "dead" links and non-related or standard menu items. Thus, it was claimed that the Website's organization was unclear and its usefulness for reporting cyber incidents was limited. On the other hand, the language toggle was useful, as it translated some features of the Website into Bangla and English if the language button was clicked. However, some features, such as "National CERT" and "Cybersecurity Training and Certification," were always in English. For departmental information, the language button feature was ineffective, as the department's information was already provided in Bangla, and the language-changing feature did not translate it into English. All these problems combined reveal both technical deficiencies (insecure security configuration, broken web components) and user experience flaws (poorly structured information architecture, missing feedback facilities) that make the DSA channel fail to act as a trustworthy digital reporting body. Ultimately, the users' verdict was "This Website was a good source of information, although some contact numbers were not helpful. However, as a cybercrime reporting website, it fell short in this aspect.(Table 4.3) (Figure 4.5)

Table 4.3: DSA Website Usability Issues Mapped to HCI Principles (Nielsen's Heuristics)

S/N	**HCI Usability Principle**	**How the DSA Website Failed to Follow HCI Principles**	**No. of Participants**
1	Visibility of System Status	Unclear response after clicking on multiple buttons	40
2	Match Between System and Real World	Use of unclear technical jargon that participants could not relate to	11
3	Consistency and Standards	Website's organization was unclear and its usefulness for reporting cyber incidents was limited	40
4	Error Prevention	Website alerted users that "this link may be dangerous," creating confusion	2
5	Help and Documentation	Helpline number either does not pick up or redirects to unhelpful numbers	7
6	Aesthetic and Minimalist Design	Designs were cluttered with too much information presented at once	6
7	Error Recovery and Feedback	Chatbot does not work and gives an "Error 404" alert	6

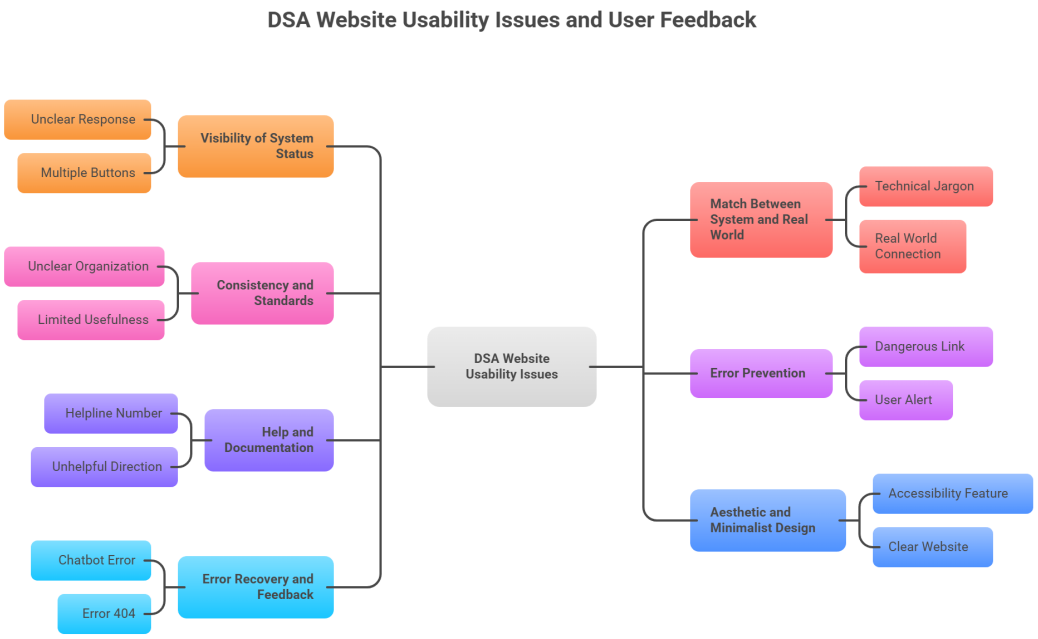

Figure 4.5: DSA Usability Issues

4.5.3 BTRC

According to users, BTRC is also a similar kind of Website to DSA. The only difference they found was that DSA provided information about cybercrime in Bangladesh, whereas BTRC is focused on information technologies in Bangladesh. While participants' experience with BTRC was generally more positive, with better-than-average sites' visual presentation and some accessibility features, significant functional gaps still existed. This Website also does not provide any complaint forms. If an individual faces any issues related to information technology, a complaint cannot be filed here. A helpline was provided, but it takes too long to connect, and it does not offer any online help. Users were also confused about using a complaint, particularly regarding the available complaint categories, the form fields' vagueness, and various unselectable and unworthy subcategories for cyber-related complaints. Without these, false, incorrect complaints could not be registered, which created a worrisome belief among them. One common thread among these seemed to be a lack of ID verification and a lack of a complaint tracking mechanism (OTP is not provided, and there is a lack of Tracking IDs), which made consumers unsure whether their complaints were being processed or who was to be held responsible for any further action. Mobile optimization was another recurring issue: form elements and pages were not displayed correctly on small screens, and repetitive pop-ups interrupted the task completion process. While a few participants liked the cleaner look of the site and working access controls, the overall interaction model did not enable successful end-to-end complaint submission: users could start submitting a report, but they could not confidently complete it or check its status — this damages both usability and credibility. (Table 4.4) (Figure 4.6)

Table 4.4: BTRC Website Usability Issues Mapped to HCI Principles (Nielsen's Heuristics)

S/N	HCI Usability Principle	How the BTRC Website Failed to Follow HCI Principles	No. of Participants
1	Visibility of System Status	Unclear response after clicking on multiple buttons	4
2	Match Between System and Real World	Use of unclear technical jargon that participants could not relate to	7
3	Consistency and Standards	Website's organization was unclear and its usefulness for reporting cyber incidents was limited	40
4	Help and Documentation	Helpline number either does not pick up or redirects to unhelpful numbers	7
5	Aesthetic and Minimalist Design	Designs were cluttered with too much information presented at once	9
6	Error Recovery and Feedback	Chatbot does not work and gives an "Error 404" alert	6

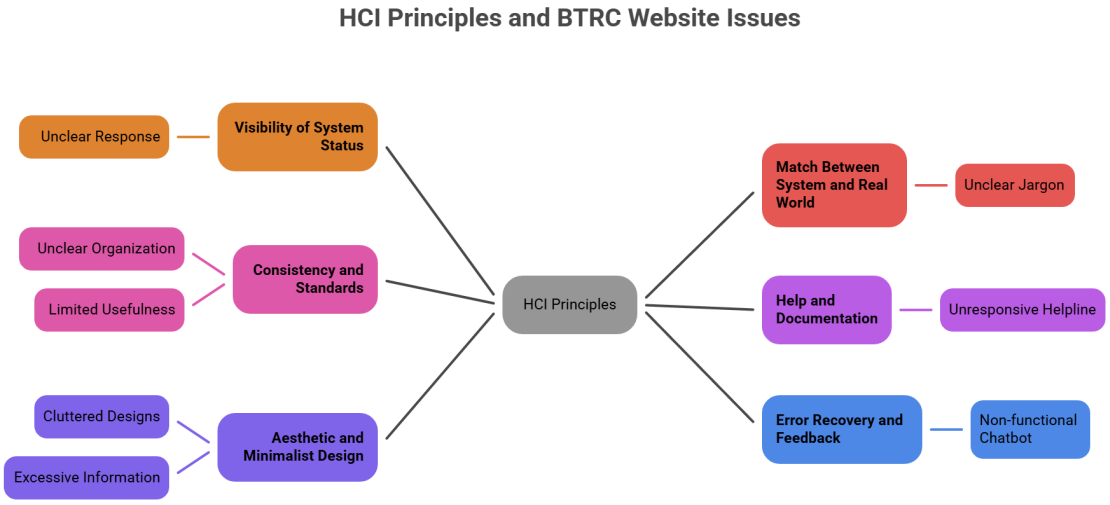

Figure 4.6: BTRC Usability Issues

4.5.4 Online GD(Mobile App)

The Online GD application had a unique set of issues that emerged during task-based assessments. Many respondents felt that the app's scope was too limited to "lost and found" or location-based goods and services, and did not have enough room for cybercrime reporting. As a result, there was no clearly defined, specific workflow for cyberbullying, financial fraud, or harassment complaints. The available complaint forms were often criticized as being too lengthy and including unnecessary questions. In contrast, the corresponding help documentation was convoluted, thereby increasing the likelihood that users did not use the app properly. The authentication and onboarding experience was great, but face-scan registration would sometimes fail, and OTP delivery was delayed or missing in some cases, resulting in friction during the account creation process. Users also stated that the app's graphical elements were too childish and unprofessional-looking, which they felt negatively

affected the perceived seriousness and credibility, particularly among older users who were expected to have difficulty with the registration flow. Importantly, the lack of transparent confirmation and tracking mechanisms (no submission codes and no visible processing status) in the app replicated issues found on the corresponding websites and contributed to a wider problem. Participants who had experience using this app stated, " The app took too much time to load and after I patiently filled up all the necessary boxes the app crashed and took me to the start again so I gave up and went to the police station." The lack of digital options for users to follow up with authorities upon submission and verify receipt of their complaints was a shortcoming in the app that reduced participant confidence in it as a viable alternative to the police station. (Table 4.5) (Figure 4.7)

Table 4.5: Online GD Mobile App Usability Issues Mapped to HCI Principles (Nielsen's Heuristics)

S/N	**HCI Usability Principle**	**How the Online GD Mobile App Failed to Follow HCI Principles**	**No. of Participants**
1	Visibility of System Status	No visible tracking system of investigation	13
2	Flexibility & Efficiency of Use	Limited scope of filing various kinds of crime — it only works for lost and found cases, ultimately asking users to visit the police station in person	19
3	Consistency and Standards	The app is not consistent. It sometimes crashes during use and forces users to refill forms	5
4	Error Prevention & Feedback	Face recognition creates issues. The app delays sending OTP codes or fails to send them entirely	3
5	Aesthetic and Minimalist Design	The forms were too lengthy for users to fill patiently, and the overall design looked unprofessional	7

Figure 4.7: Online GD Usability Issues

4.5.5 Cross-platform synthesis and HCI implications

From all the platforms investigated, several common themes emerged, explaining why users abandon activities or distrust online reporting services. First, poorly conceived information architecture and crammed homepages hinder findability: users cannot easily find complaint forms or relevant pathways without extensive searching, and site search mechanisms are not forgiving (they have spell-checks or query suggestions to help non-expert users). Second, the lack of confirmatory feedback and validation, such as no confirmation, no tracking, and no identifiable validation, makes the heuristic of system status non-visible and diminishes credibility. Users reiterated their desire to report online but in person due to the lack of confirmation and follow-ups. Third, faulty interactive elements (such as chatbots, help links, form fields, and back-button navigation) and security warnings create trust gaps. Fourth, the lack of accessibility and localization features, such as poor and unreliable language switching, the lack of mobile-friendliness, and the absence of assistive technology support, excludes large groups of users and is contrary to the core principles of inclusive design. Finally, the platforms are low error-tolerant and poor at error recovery, displaying obscure or technical error messages, missing guidelines, and non-descriptive failures, which force the user into workarounds or abandonment.

Collectively, these results show that usability failures are not isolated. Qualitative evidence from think-aloud transcripts, body language, and post-task interviews confirms that these technical and interaction failures are reflected in emotional responses (frustration, mistrust, resignation), which can discourage public adoption if the platforms are not redesigned to accommodate users' expectations and usability heuristics better.

4.6 Result

Usability testing has provided us with a rich understanding of how Bangladeshi users perceive and interact with government digital platforms for reporting cybercrime. Despite being experienced internet users, sixteen participants who also had a computer science background or were related to technology faced numerous obstacles throughout various points of interaction. The results are organized according to the Honeycomb User Experience Model, which encompasses findability, usability, credibility, usefulness, desirability, and value.

To quantify the magnitude of these problems, we turned the frequency for each question into percentages as follows:

$$P = \frac{n}{N} \times 100$$

Here:
P = Percentage of users affected
n = Number of participants reporting that particular issue
N = Total Number of participants
(Table 4.7)

Additionally, two other parameters were also considered: the Severity Index (SI), which accounts for the weight of each issue in relation to task criticality, and the Error Rate (ER), which represents the Number of misattempts divided by the total Number of attempts. These measures ensured fair assessment of specific problems, as well as their impact on critical user tasks, such as filing complaints.

Findability

The first obstacle was finding the reporting sites and then navigating within them. Fourteen(16) participants had previous experience with government digital platforms. However, twelve (12) reported difficulty finding the target sites unaided, and six (6) did not find them at all without assistance from facilitators. For another young, tech-savvy participant, a 23-year-old student of Computer Science at BRAC University, it took him just 19 minutes to navigate from a blank browser page to the Online GD platform, providing insight into how challenging this is for everyone else.

Participants strongly agreed that the searching feature in the Online GD app was not always up to date.

> "The provided search feature was especially frustrating. Sometimes it showed an error 404 if I typed something here." - Female, 21, Bachelor of Laws, North South University.

Participants noted that the results were often irrelevant to their needs and that they received lengthy lists of documents with no enhanced features, such as spell checking or synonym support, which are typically provided in commercial search engines. The situation was especially bad for non-native English speakers.

> "I typed 'online harassment' so many times, but the results never gave me the form or gave any guidance on what I should type to get it. It was frustrating so I gave up." – Male, 23, BRAC University.

The Error Rate (ER) for search queries can be calculated as:

$$ER = \frac{\text{No. of failed searches}}{\text{Total Searches Attempted}} \times 100\%$$

A total of 37 searches were attempted among the 40 users, and among them, 14 searches did not yield any results or displayed a 404 error message.

$$\begin{aligned} \text{No. of failed searches} &= 14 \\ \text{Total Search attempts within platforms} &= 37 \\ ER &= \frac{14}{37} \times 100\% \\ &\approx 37.838 \end{aligned}$$

This measure indicates how often participants were unable to retrieve meaningful content for their query, thus highlighting flaws in the site's search structure.

Usability

When the websites were found, further usability problems arose in accessing the domains for further evaluation. Technical language, tiny fonts (for some users), and cluttered designs made simple navigation a very challenging task for all users. Crucial information, such as where to find the cybercrime complaint form, was buried beneath a heap of irrelevant material. Users frequently struggled with their starting point and the subsequent steps.

A 24-year-old Business Studies student of United International University said,

> "The form was there, but put in such a place that I just about gave up. If it were not for a test, I'd have already been off the site."

Moreover, NSU's female student, also aged 27, in Public Health, said,

> "The writing is too small and technical. It feels like it's a site for officials, not for a regular user like me."

To quantify the time overweight from these design failures, we calculated Mean Time to Task Completion (MTTC) as:

$$MTTC = \frac{\sum t}{n}$$

Where:
$\sum t$ = total time spent by all participants attempting all tasks in the CID and online mobile GD app (in minutes)
n = total participants

Total Time ($\sum t$) = 616 minutes (rounded time)
Number of Participants (n) = 40

$$\begin{aligned} MTTC &= \frac{\sum t}{n} \\ &= \frac{616}{40} \\ &= 15.4 \end{aligned}$$

So, in conclusion, we can assume time = 15.4 minutes (approximately).

Credibility

To report a crime, one must first trust a website or system, as users will be sharing their personal information. This is why users would go to a government-issued site, as it should be a trustworthy source. However, the CID site itself lost credibility due to poor brand management, which contradicted who was accountable. Pages frequently went through external or interlinked government portals. Participants had no way of knowing if the data collected was being protected.

> "I thought the government checks all sites here, but later I found out that many links just go elsewhere." - A 31-year-old male doctor at Shaheed Suhrawardy Medical College & Hospital.

These trust issues directly influenced the amount of personal information users were willing to provide.

> "If I put my information here, like NID number or some confidential documents which might be needed for investigation purposes, who will be navigating them? I was confused and doubtful at that part, you see?" - Female, 28, Nurse from NICVD.

To measure how bad an issue is, we use the Severity Index (SI):

$$SI = \frac{n}{N} \times W$$

n = Number of participants who reported the issue
N = total Number of participants

W = weight representing how critical the issue is

Severity Index Interpreter (SI)
(Keeping in mind that W is from 1 to 3 scale)

- 0.0 – 0.5 → Low severity (minor inconvenience, cosmetic issues).
- 0.5 – 1.5 → Medium severity (affects usability, but not task completion).
- 1.5 – 3.0 → High severity (major usability failure, trust/security problem).

W = 3 (Critical) — Issue prevents task completion, risks user privacy/security, or causes major loss of trust (example: no secure submission, data leak).
W = 2 (Major) — Issue significantly slows users, causes frequent errors, or causes serious confusion (example: not finding the complaint form, broken navigation).
W = 1 (Minor) — Cosmetic, small annoyances, or usability degradations that do not block tasks (example: small font size, minor wording).(Table 4.6)(Figure 4.8)

Table 4.6: Identified Issues and Severity Index (SI)

Serial No.	Issue Identified	Number of Participants Pointing Out These Issues	Weight (W) (1-3)	Severity Index (SI)
1	Cluttered Website with much information at once (Design Issue)	40	2	2
2	Not finding the complaint form. (For two website forms do not exist)	38	2	1.9
3	No confirmation or tracking ID of the filed complaint	13	3	0.975
4	The complaint form was taken to another interlinked website, which confused users (CID)	29	2	1.45
5	The Search Engine is not working properly	7	2	0.35
6	Inconsistent language, sometimes not working properly	13	1	0.325
7	FAQ: Features not working	17	1	0.425
8	Flexibility and no efficiency or shortcuts to features	3	1	0.075
9	Confusing forms, not being able to understand what the form actually wants	29	2	1.45
10	The helpline number is either busy or not picking up at all	9	1	0.225
11	Privacy issue as not knowing where the complaint form has been submitted	14	3	1.05
12	No proper login system, anyone can come and submit a fake report	17	2	0.85
13	Needing a proper chatbot or a similar kind of feature	23	1	0.575

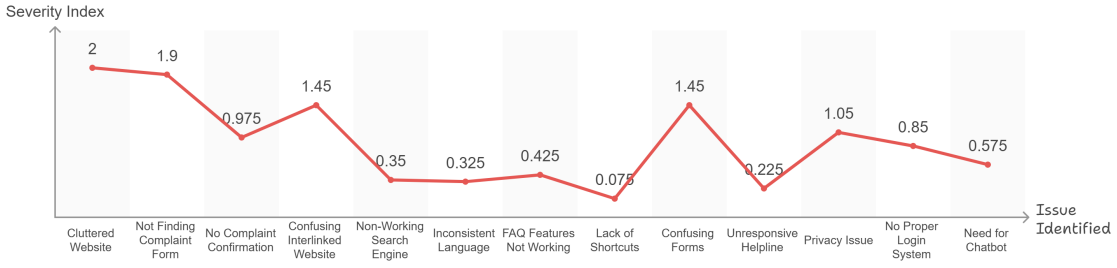

Figure 4.8: Severity Index of Website Issues

Usefulness

Participants expected personalized, actionable content from the platforms. However, users encountered generic information and received minimal guidance on navigating the processes applicable to different user types. For users who expect a cybercrime

reporting system or online gaming, these websites would be fast, feature a tracking system, and offer a superior user experience design. However, they met with the same old, confusing UX. Information is scattered, and the systems are handling everything except the actual tasks, which were to receive crime reports from users and resolve those.

Desirability

The Website was described by users in all communities as generally disordered, confusing, and unpleasant. There was no modern response design, and the information was overwhelming for most people, including tech-savvy users.

> "The Website looks aged and complicated. I do not think they design these systems for regular people like us."

Many users have let us know about their disappointment with their expectations of modern life websites. They expected more from a website operating in the 21st-century era. According to this timeline, the platform the government is providing us is old-fashioned, even compared to other countries' government sites.

Value

The reduced findability, usability, and credibility of these platforms influenced the perceived value of the stated platforms. Participants wondered whether these systems were worth the investment of time and trust.

> "I agree, the police station is such a hassle, and personally, I do not like to go there, but over these broken websites, I would like to take the police station hassle," a 37-year-old doctor said sarcastically.

> "These systems, especially the CID and online GD mobile app, were supposed to save me time, but I am skeptical about how they are actually saving my time. Even for user testing with dummy data, it gave me a headache. I cannot even imagine using these if I had an actual issue to complain about," - Male, 31, Intern software engineer.

From these statements, we can conclude that users agree that police stations are inconvenient, but using these systems over police stations is no better. In some cases, people prefer to visit a police station in person rather than using this system. Additionally, a 36-year-old female banker stated,

> "For financial fraud issues, I must go to the police station, as I will not disclose my personal, confidential data here online that might put me in further danger."

These stories illustrate that although the potential of a functional online reporting system is appreciated, it has yet to be realized through the present format.(Figure 4.9)

Table 4.7: Summary of Findings and Recommendations

Category	**Problem Identified**	**Percentage (%)**	**Suggestions for Improvement**
Navigation	Menus are disorganized and have redundant steps.	100	Dynamic system design should present logical groupings of features along with menu simplification.
Navigation	Users encounter barriers when they attempt to access critical features.	67.5	The system should include easily accessible links to emergency reporting together with tasks that require immediate attention.
Design & Layout	Every interface element shows signs of age while being suboptimal for mobile user experiences.	72.5	Design improvements should bring modern updates, which guarantee consistent and responsive functions for mobile users.
Design & Layout	Overcrowded pages with irrelevant information.	100	The interface can be simplified through the organization of meaningful content while using visual hierarchy principles.
Forms for complaints	Forms presented difficulties due to missing components, advanced complexity levels, and technical errors.	77.5	Your system should offer easy-to-use forms together with clear instructions and automated error detection systems.
Forms for complaints	No acknowledgment after form submission.	22.5	The system needs to display both a submission confirmation message and assignment of tracking IDs after user submissions.
Security	Complaint submitters lack verification, which creates doubts about the platform reliability.	16	Users must authenticate with National Identity Card credentials and enter One-Time Passwords for verification.
Security	Insufficient encrypted data protection leaves stored data vulnerable to security threats.	7.5	For all transactions implementing encryption along with SSL certification, the platform should be secured.
Search Feature	The system lacks an accessible search function.	17.5	A simple search interface would be helpful for broader users to enhance their discovery of items.
Crime Reporting	Users cannot submit Cyberbullying or harassment reports are categorized under reporting categories.	32.5	Expand the classification range to encompass all standard cybercrime scenarios.
Speeds for loading pages	Slow page load times, especially for image-heavy pages.	27.5	Pages must contain optimized images and code to enhance delivery speed, particularly across mobile platforms.
Error Handling	Error messages were technical and unclear language, which angered users as they tried to understand the issue.	52.5	Users need clear solutions, along with precise instructions, to resolve system errors.

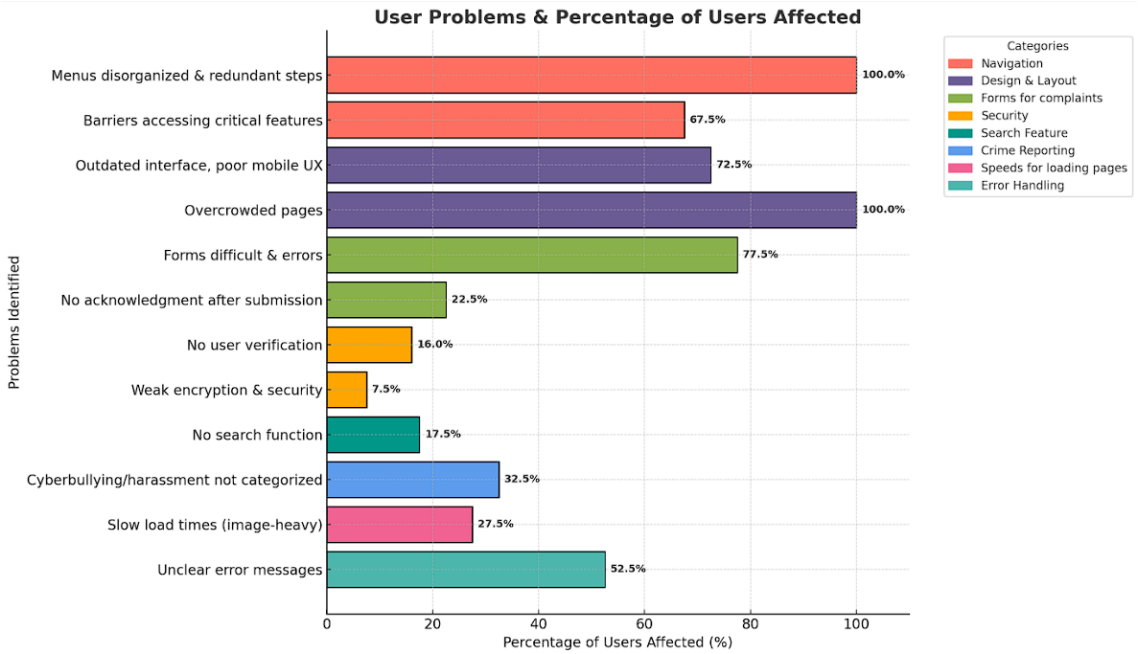

Figure 4.9: User Issues in Percentage

4.7 Recommendation (From User Perspective)

The recommendations gathered during the evaluative phase form the basis for creating a credible and widely adopted cybercrime reporting system. From numerous in-person and online focus group sessions, participants identified common themes that served as a foundation supporting an effective platform: trust, accessibility, ease, and guidance. Fourteen participants, including many professionals working with IT and students, called for the introduction of a verified registration system using National ID numbers or birth certificates. A 30-year-old IT technician asked,

> "Otherwise, how would we know this is a verified website? The government actually verifies the users, and the issues complained are going to verified admins."

Verification was considered not as an impediment, but as an indispensable requirement to establish authenticity and legitimacy. A general call for simplified filing of complaints was expressed uniformly by participants. All respondents expressed frustration with the overly complicated requirements, which were more tiresome than going to the police station in person. Instead, they devised a streamlined form to enable victims to submit initial complaints without requiring exhaustive documentation. A 24-year-old student majoring in Business Studies said,

> "When I can simply just go to a website and file a complaint and solve an issue, then I would love to use it. However, the reviews of the Website should be there for me to trust the site."

The need for tracking the investigation process became another important theme. Nine participants explicitly requested an acknowledgement system, such as a confirmation email, SMS message alert, or updates about the status of their complaints.

Others did not request directly but indicated that some confirmation would be better for them. A 21-year-old female participant stated,

> "If I were to know that my complaint had been received and was under investigation, I would feel at ease."

Requests for interaction and guidance were also constant. Twenty-three people supported adding either a chatbot or live helpdesk feature, especially to offer assistance to those who are less technologically savvy. Concurrently, thirty-four called for step-by-step guidance that provides navigation information in both Bangla and English. A 36-year-old banker, who was an official, said,

> "If there were a guideline in Bangla and English, then it would save so much time for so many users. Not everyone is comfortable navigating a website in English, as there would be technical terms included."

Clarity of content was also emphasized. Nine respondents expressed a need for online training that addresses the different types of cybercrime. Also the need of these guidance in two languages, that would make the digital systems more inclusive to the wider community. Twenty-six people expressed a clear preference for a well-designed online reporting mechanism over dealing with a police station, particularly for incidents of online harassment, abuse cases, and social media issues.
However, three bankers and one person who had personally been a victim of financial fraud, stated more complex offences, such as credit card fraud or unauthorized access to banking accounts, that could only be directly addressed in person. A 27-year-old female victim stated,

> "From a Bangladeshi perspective, sharing confidential information such as credit card info online is quite scary for me personally. For financial fraud, I won't use online websites. However, the rest I might rely on them."

The combined user testing results suggest that users are prepared and willing to adopt digital cybercrime reporting tools if the platforms guarantee safety, reliability, authenticity, proper usability, transparency, and an ongoing commitment to these values are met. In the absence of these key elements, the perception that physical police stations are more reliable due to their inefficiencies is reinforced.

Chapter 5

Heuristic Evaluation

Heuristic evaluation establishes itself as a crucial tool for identifying user interface usability issues. Through this method, organizations obtain systematic insights that help them identify design issues alongside possible solutions. The analysis evaluates ten usability heuristics developed by Nielsen, assessing vital aspects of the system's user status, platform interaction with real-world systems, user-controllable elements, error-preventing factors, and other key areas [7]. The goal of this heuristic evaluation is to enhance usability features, accessibility standards, and user-friendly functionality across the Criminal Investigation Department (CID) website, the Bangladesh Telecommunication Regulatory Commission (BTRC) website, as well as the Digital Security Act (DSA) platform and the Online GD application in Bangladesh.

5.1 Evaluator Expertise

A research group consisting of Sohayab, Omar, Neha, Taskia, and Anika conducted the assessment because we possess extensive experience in Human-Computer Interaction (HCI), Software Engineering, and System Analysis and Design. Five evaluators contribute to the assessment, bringing practical expertise in usability testing, interface prototyping, and user-centered design practices. The evaluators employed academic coursework, along with practical experiences, to analyze real-world usability issues in applications as well as conduct user studies while implementing sequential design upgrades. The experience enables us to perform thorough assessments of the chosen Cybercrime reporting systems.

5.2 Evaluation Methodology

In this chapter, we basically discuss the technique and method of heuristic evaluation. This technique is widely recognized by researchers in human-computer interaction as a method of systematically discovering usability problems by means of expert analysis [48]. By applying ten heuristics of user experience proposed by Nielsen as principles, evaluators were able to go beyond the established usability standards to determine the extent to which the platform falls under them. This was achieved through an orderly observation, self-assessment, rating of the severity of problems, and collective discussion of results to ensure the richness and validity of the findings [49].

5.2.1 Heuristic Selection and Criteria

The evaluation used Nielsen's ten usability heuristics for UX analysis [7]. These heuristics include:

1. **Visibility of System Status:** Users should receive feedback and updates about system.
2. **Match Between System and the Real World:** System language and structure should align with user expectations. And also, with the real-world.
3. **User Control and Freedom:** Users should be able to undo and redo actions and navigate freely within the application.
4. **Consistency and Standards:** Terminology, navigation structures, and interface elements should be consistent across the platform.
5. **Error Prevention:** The system should minimize the chance of user.
6. **Recognition Rather Than Recall:** The important elements should be visible and user don't have to remember information.
7. **Flexibility and Efficiency of Use:** The system should support expert users through shortcuts and customization.
8. **Aesthetic and Minimalist Design:** The interface should present relevant information clearly and avoid unnecessary content.
9. **Help Users Recognize, Diagnose, and Recover from Errors:** Error messages should be clear, informative, and guide users to resolve issues.
10. **Help and Documentation:** Support features such as FAQs, tutorials, and guides should be readily accessible.

5.2.2 Evaluation Procedure

The heuristic evaluation followed a structured procedure: **Platform Introduction:** Evaluators explored platform functionalities, user targets, and operational procedures. **Independent Heuristic Assessment:** Each evaluator individually assessed the platforms against the ten usability heuristics and documented issues. **Severity Rating Assignment:** Each identified issue received a severity rating from 0 to 4:

0 – No usability problem

1 – Cosmetic problem only

2 – Minor usability problem

3 – Major usability problem

4 – Usability catastrophe

Consensus and Discussion: Evaluators discussed and resolved disagreements to refine findings. **Graphical Representation:** Graphs were used to visualize severity ratings across platforms.

5.2.3 Data Collection and Documentation

The team used detailed observation notes, screenshots, and user interaction evidence. Usability issues were classified under Nielsen's heuristics and documented with severity ratings and proposed solutions.

5.3 Findings and Usability Issues

This section summarises the primary usability issues identified across BTRC, CID, DSA, and Online GD platforms. The findings are presented in terms of Nielsen's usability heuristics, including system feedback, language clarity, control, consistency, error handling, and support environment. Each issue identifies gaps and the resulting lack of efficiency, accessibility, and user satisfaction before suggesting enhanced user experience[50].

5.3.1 Visibility of System Status

The BTRC, CID, DSA, and Online GD app lack real-time system feedback. Users do not receive confirmation messages or status updates after submitting forms. For example, Online GD users are unsure whether their data has been received. The platforms need visual feedback, progress indicators, and submission time stamps to improve user confidence. (Figure 5.1)

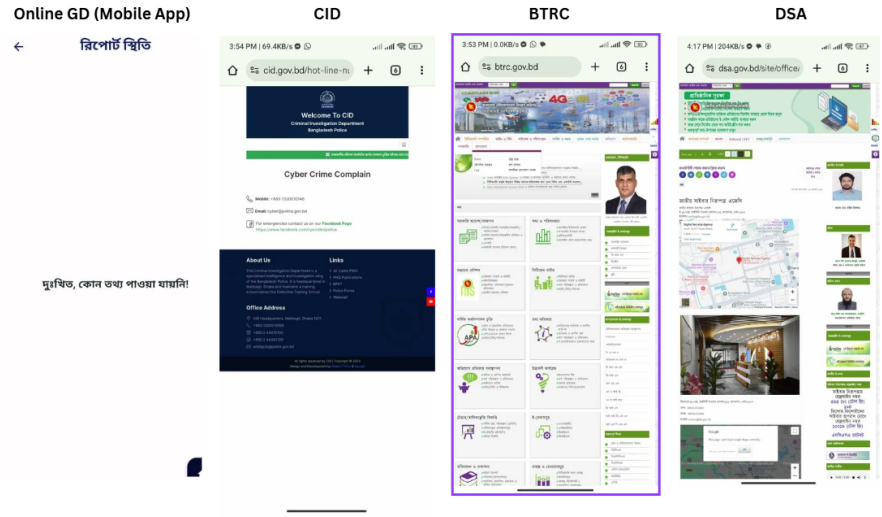

Figure 5.1: Visibility of System Status

5.3.2 Match Between System and the Real World

For instance, BTRC and CID use terms like "incident escalation" and "General Diary" without clarification. The DSA platform includes cybersecurity jargon that can confuse users. The Online GD app, while in Bengali, lacks options for non-Bengali speakers. Simplifying terminology and offering multilingual support can improve user comprehension. (Figure 5.2)

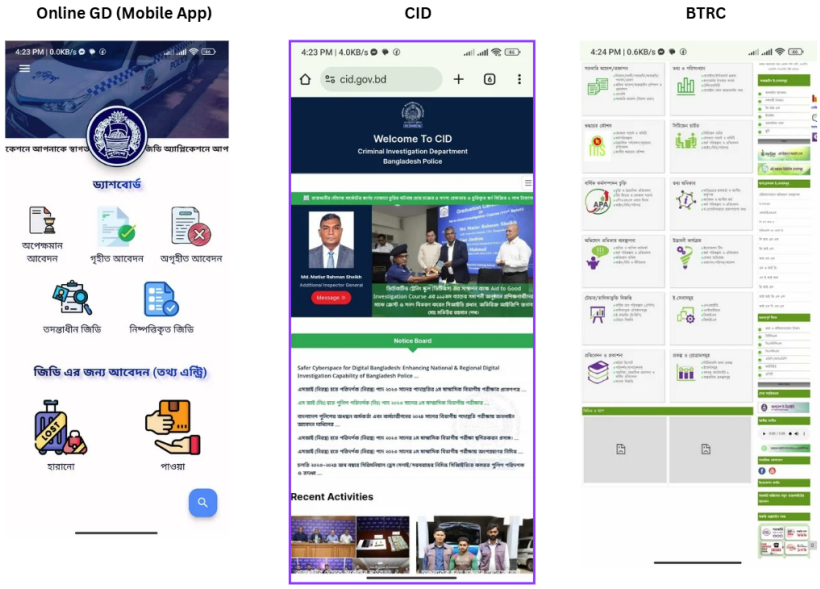

Figure 5.2: Match Between System and the Real World

5.3.3 User Control and Freedom

These platforms provide limited options to undo actions or navigate freely. Online GD users cannot edit or withdraw submissions. The DSA platform lacks back navigation options. Adding "Undo," "Edit," and "Cancel" features, as well as autosave options, would significantly improve user satisfaction. (Figure 5.3)

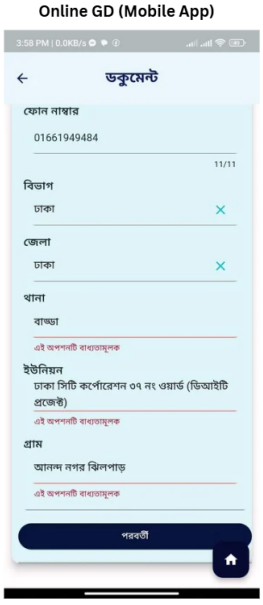

Figure 5.3: User Control and Freedom

5.3.4 Consistency and Standards

Platforms exhibit inconsistent terminology and layouts. BTRC uses varied navigation styles across pages, and CID labels similar functions differently. DSA displays inconsistent design elements across pages. Adhering to a unified style guide would improve navigability and reduce learning time. (Figure 5.4)

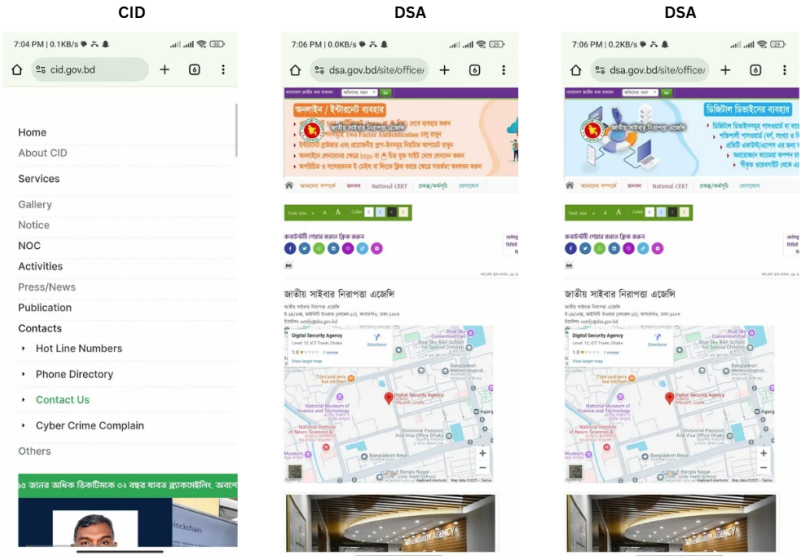

Figure 5.4: Consistency and Standards

5.3.5 Error Prevention

All platforms fail to proactively prevent errors. BTRC allows submission of incomplete forms. The Online GD app lacks prompts before deleting content. CID does not validate inputs before submission. Implementing input validation, confirmation prompts, and clear field instructions can reduce user errors [7]. (Figure 5.5)

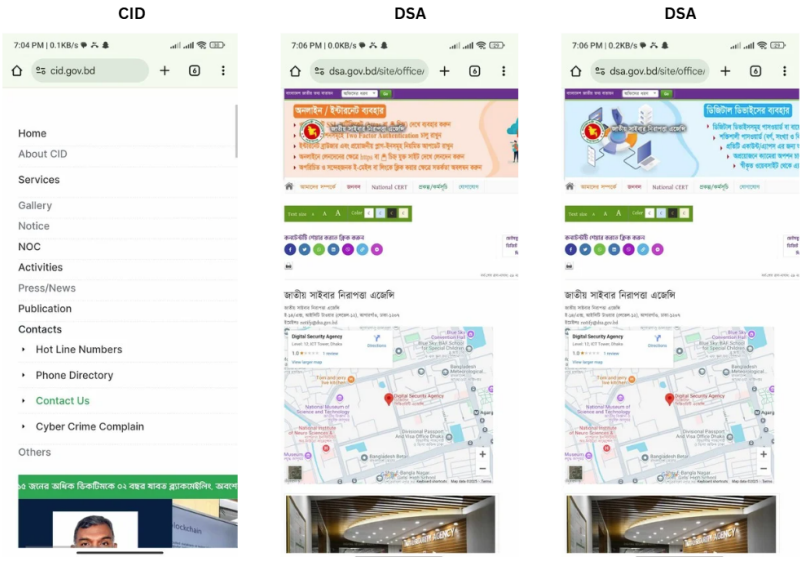

Figure 5.5: Error Prevention

5.3.6 Recognition Rather Than Recall

Platforms demand users recall prior inputs or navigation paths. CID hides essential contact information under deep navigation. The Online GD app does not save data or offer autofill. BTRC navigation requires memorization. Using breadcrumbs, autofill, and clearly labeled buttons can ease cognitive load. (Figure 5.6)

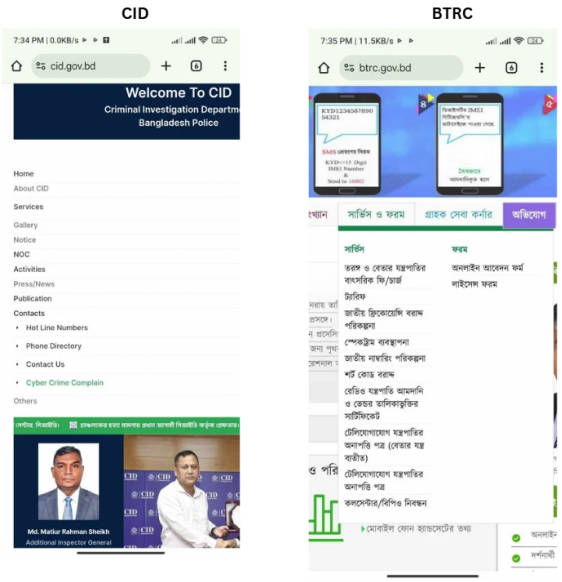

Figure 5.6: Recognition Rather Than Recall

5.3.7 Flexibility and Efficiency of Use

Platforms lack features for both novice and experienced users. Online GD lacks templates for repeated use. BTRC has limited search functionality, and DSA lacks filters. Adding advanced search, shortcuts, saved preferences, and dashboards would support efficient navigation. (Figure 5.7)

5.3.8 Aesthetic and Minimalist Design

Interfaces are cluttered and text-heavy. BTRC repeats links, CID lacks visual hierarchy, and Online GD uses outdated layouts. Prioritizing important content, using whitespace, and applying consistent color themes would improve visual appeal and comprehension.

5.3.9 Help Users Recognize, Diagnose, and Recover from Errors

Error messages are vague and unhelpful. For example, BTRC and DSA display "Error occurred" without explanations. Online GD forces resubmission on errors. CID lacks guidance. Detailed error messages with actionable steps and color-coded field highlights can enhance recovery.

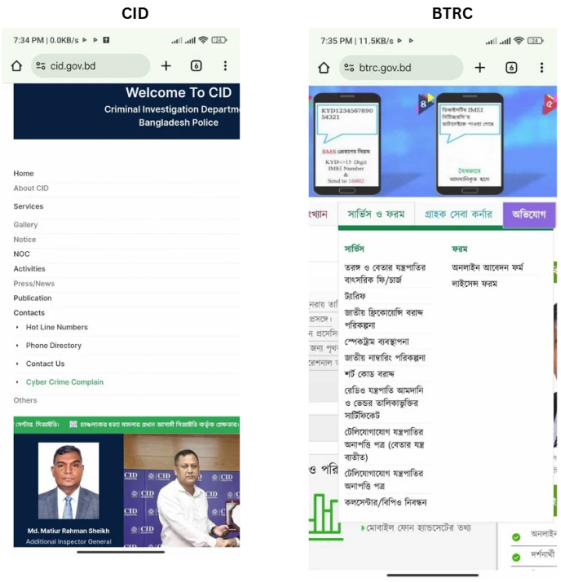

Figure 5.7: Flexibility and Efficiency of Use

5.3.10 Help and Documentation

Support content is minimal across all platforms. The Online GD app, BTRC, CID, and DSA lack FAQs, tutorials, and guides. Providing centralized help sections, video walkthroughs, and live chat/email support will improve user onboarding and trust. (Figure 5.8)

.

5.4 Graphical Representation

This section provides the summary of the heuristic evaluation results graphically to visually compare usability challenges of the cybercrime reporting platforms (CID, BTRC, DSA, and Online GD). Severity ratings of each heuristic are presented in the below table whereas the radar chart shows trends in usability performance.

5.4.1 Heuristic Evaluation Summary Table

The results presented in the following table (Table 5.1) show the severity rating for each heuristic in the evaluated platforms. The latter describes the severity levels as 0 (No issue) to 4 (Critical usability problem). Each heuristic is summarized with key usability issues.

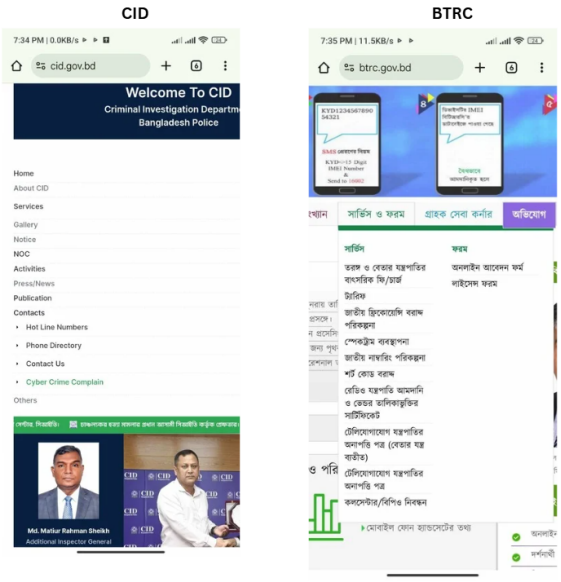

Figure 5.8: Aesthetic and Minimalist Design

Table 5.1: Heuristic Evaluation Summary Table

Heuristic	CID	BTRC	DSA	Online GD	Key Issues Identified
Visibility of System Status	2	4	2	1	Users do not see confirmation messages and cannot track any progress
Match Between System & Real World	2	2	2	3	Specialist terms and official language that normal users may find difficult to understand
User Control & Freedom	1	2	1	2	Few ways to reverse actions or fix errors, no feature to edit or withdraw submissions
Consistency & Standards	2	2	3	2	Inconsistent terminology, navigation elements shift inconsistently across screens
Error Prevention	2	1	3	2	No adequate error-prevention mechanisms, allows form submission without validation
Recognition Rather Than Recall	2	2	3	2	Users must remember too much information, lack of autofill or memory-saving features
Flexibility & Efficiency of Use	3	4	4	3	Repetitive data entry, no templates or saved entries, lacks advanced search and filters
Aesthetic & Minimalist Design	1	3	3	1	Excessive content in cluttered layouts, difficult for users to navigate
Help Users Recover from Errors	1	3	1	2	Basic and unclear error messages, no correction option, no troubleshooting support
Help & Documentation	3	3	2	2	Lacks extensive support resources, minimal or no FAQs, user guides, or instructions

5.4.2 Radar Chart Visualization

Below is a radar chart (Figure 5.9) which compares heuristic ratings of each platform. The radar chart consists of each usability heuristic on an axis and the closer a platform's score is to the outer edge, the better the usability performance. Lower is better as it indicates significant usability issues.

Key Insights from the Visualization

From the table, radar chart, and bar chart, we can conclude the following:

- Low scores in "Error Prevention" and "User Control & Freedom" imply that most of the platforms lack undo/cancel options and proper error validation.
- Users are not provided with enough feedback about system processes, as shown by the poor scores in "Visibility of System Status" across all platforms.
- Although using Bengali led to slightly better performance in "Match Between System and Real World" (as expected since the real-world data was collected

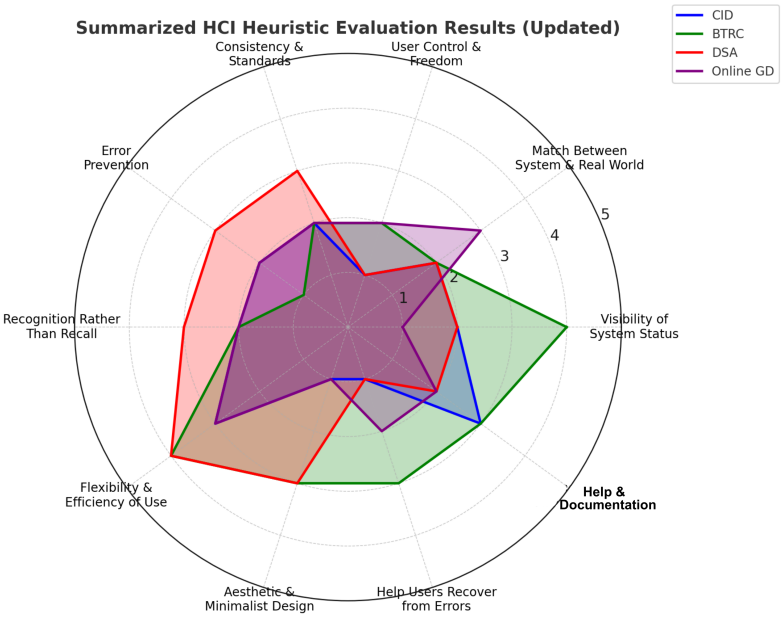

Figure 5.9: Radar Chart of Heuristic Evaluation Results

from the same population), it also made the system inaccessible to users who did not know Bengali.

- All platforms exhibit "consistency issues", as evident from the low scores in "Consistency & Standards".

5.4.3 Cumulative Frequency Graph

This ogive curve (Figure 5.10) represents the cumulative severity rating of the usability heuristics in the four different platforms: CID, BTRC, DSA, and Online GD. The x-axis can be seen as the ten usability principles tested, and the y-axis can be seen as the cumulative severity measure (individual rating of heuristics) (0-4 scale).

The curve represents the accumulation of usability problems in various categories of heuristics. The steeper the slope, the more the issue of the platforms will be concentrated in the heuristics, and the more even in the flatter slopes. The BTRC platform displays the most acute increase at the beginning of the heuristic sequence, indicating that usability issues were especially severe in the early phases of the system, whereas Online GD exhibits a more gradual progression of problems.

Calculation Methodology
The following formula was used to calculate the cumulative severity values:

$$C_i = \sum_{j=1}^{i} S_j$$

Here, C_i is the cumulative severity at heuristic i, and S_j is the severity rating (0-4) for heuristic j.
For example, for the BTRC platform:

- Heuristic 1 (Visibility): 4 → Cumulative: 4
- Heuristic 2 (Match): 2 → Cumulative: 4+2=6
- Heuristic 3 (Control): 2 → Cumulative: 6+2=8
- Heuristic 4 (Consistency): 2 → Cumulative: 8+2=10
- Heuristic 5 (Error Prevention): 1 → Cumulative: 10+1=11
- Heuristic 6 (Recognition): 2 → Cumulative: 11+2=13
- Heuristic 7 (Flexibility): 4 → Cumulative: 13+4=17
- Heuristic 8 (Aesthetic): 3 → Cumulative: 17+3=20
- Heuristic 9 (Recovery): 3 → Cumulative: 20+3=23
- Heuristic 10 (Documentation): 3 → Cumulative: 23+3=26

All the platforms followed the same procedure, generating cumulative progression curves that could be used to achieve a comparative analysis of the overall severity of usability problems and their distributions.

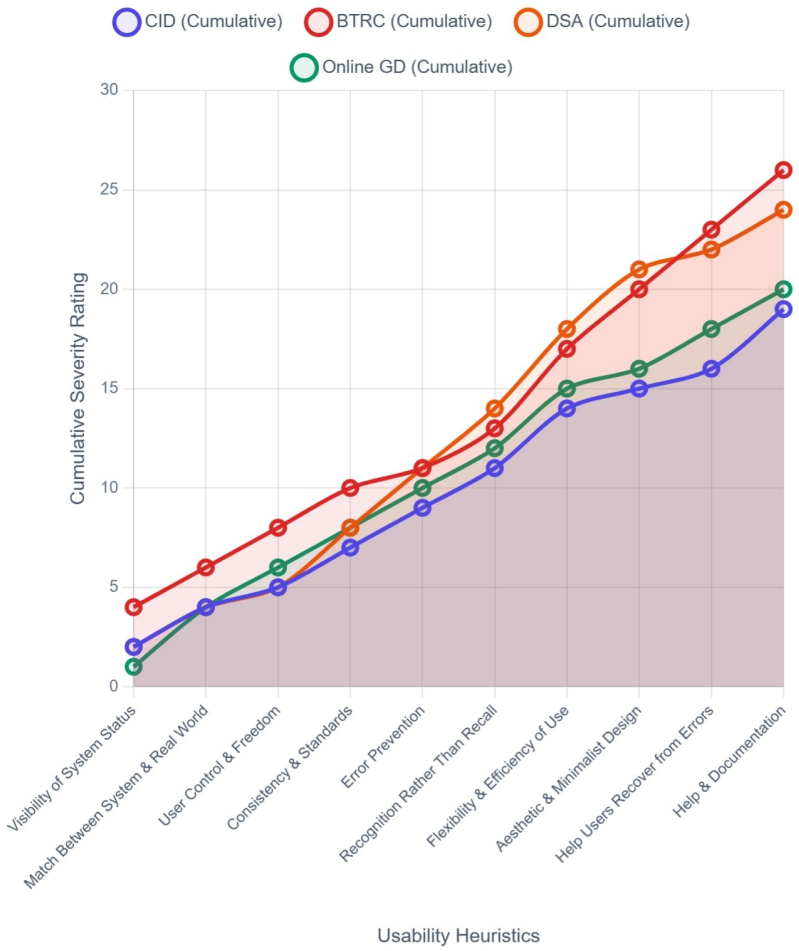

Figure 5.10: Ogive Curve

Interpretation & Significance

The analysis of this ogive curve shows (Figure 5.10) some clear trends in the accumulation of usability issues on platforms. BTRC is the most severely cumulative (26) and thus presents the most serious challenges in usability, especially in the earlier heuristics. CID exhibits the least rapidity of the course, indicating comparatively smaller serious problems. The inflection points on each curve indicate the areas on the curve where usability issues are most concentrated, and these areas can serve as a focus point for design improvement.

This methodological strategy enables both quantitative comparison of overall usability (using final cumulative values) and qualitative analysis of problem distribution patterns (using curve progression), which may be informative in prioritizing usability improvements across various platforms.

Chapter 6

Semi-Structured Interview

The chapter provides the qualitative facet of our study, namely, semi-structured interviews with the key stakeholders that work within the cybercrime-reporting ecosystem in Bangladesh. We describe the design and method of interviews, indicate the participants and their roles and provide a thematic synthesis of operational, technical and usability implications collected in law-enforcement and related institutions. The chapter subsequently summarizes emerging recommendations and records feasible issues, which limit the present reporting processes. All these findings, along with heuristic analysis and user testing, complement one another, and feed directly into the design decisions and policy-level proposals that will be made later in the thesis.

6.1 Study Design

The study collects qualitative information on the cybercrime reporting sites in Bangladesh using semi-structured interviews. Semi-structured interviews enable the researcher to have a flexible and at the same time systematic way of answering their research questions [51]. In this approach, the researcher can probe deeper, thus they can tailor questions as per the response of the respondents [51]. The approach was selected as it was necessary to get specific information about the usability of cybercrime reporting mechanisms in Bangladesh. Its form of flexibility allows the identification of important themes and consistency in analysis and allows meaningful comparisons [52]. The interviews with law enforcement agencies were also crucial to the present study since these stakeholders are the actors in the cybercrime-reporting system. Their personal, objective observations assist in detecting the operational gaps and challenges of use, as well as determining the areas of improvement. Law enforcement agencies have a major role in closing the divide between cybercrime victims and the justice system. They provide information about technical and procedural problems, how users act in the context of reporting, and the credibility factors that contribute to the overall socio-technical environment of cybercrime reporting in Bangladesh.

6.2 Participant Recruitment and Demographics

Overall, five respondents were interviewed, holding different positions and specialties: an official of the National Security Intelligence (NSI), a Sub-Inspector of the Dhaka Metropolitan Police (DMP), two representatives of the Security Solution Implementation Department of the Bangladesh Financial Intelligence Unit (BFIU), and one of the DMP Cybercrime Unit. These respondents offered valuable information related to the technical, procedural, and operational issues of present cybercrime reporting systems in Bangladesh. Below is a table (Table 6.1) summarizing the demographics of the participants:

Table 6.1: Demographics of Interview Participants

Gender	**Age**	**Organization**	**Position**
Male	35	National Security Intelligence (NSI)	Official
Male	32	Dhaka Metropolitan Police (DMP)	Sub-Inspector
Male	38	Bangladesh Financial Intelligence Unit (BFIU)	Representative (Security Solutions)
Male	33	Bangladesh Financial Intelligence Unit (BFIU)	Representative (Security Solutions)
Male	42	Dhaka Metropolitan Police (DMP) Cybercrime Unit	Officer

6.3 Interview Procedure

This section details how the interviews were carried out in practice and how the semi-structured protocol was applied. It first outlines the end-to-end data collection workflow—from briefing and informed consent to scheduling (in-person or secure online), rapport building, language choices (Bangla with English for technical terms), recording and field notes, and anonymization and storage (Section 6.3.1: *Data Collection Process*). It then presents the phased interview guide used during sessions, including exemplar prompts for consent and privacy, duration, initial awareness, deeper probing, and closing feedback (Section 6.3.2: *Sample Interview Questions*). Together, these subsections make the interview procedure transparent and reproducible for future studies.

6.3.1 Data Collection Process

We provided a plain-language brief about the study, which covered the study purpose, estimated duration of participation, and measures to keep the information confidential, and we obtained informed consent prior to each session. Interviews were subsequently arranged at a time and place suitable for participants, or via secure online conferencing, according to participant availability and the sensitivity of topics. Each session began by establishing rapport and explaining that participation was voluntary and that any question could be declined. We used a semi-structured guide that moved from general thoughts on the current cybercrime-reporting process to operational, technical, and user-experience issues; open-ended probing helped define examples as well as workflows. The sessions lasted 30-40 minutes and were

conducted in Bangali although English had to be used where technical terms were required. We recorded the sessions with permission and also made brief field notes. No information about individuals was collected in the form of personal information, and all IDs were anonymized at the processing and analysis stage. Lastly, at the end of every interview, the respondents were requested to inquire whether there were any other issues or suggestions they previously did not address, and they were informed that their feedback will be utilized to make cybercrime-reporting tools more usable and effective.

6.3.2 Sample Interview Questions

The semi-structured interview questions were designed to guide the discussion through different phases, ensuring that all relevant aspects of the cybercrime-reporting process were covered. These phases included initial consent, establishing the interviewee's awareness of the reporting system, probing deeper into specific experiences, and concluding with feedback on potential improvements.
(Table 6.2) presents the sample interview questions categorized by phase, highlighting the structure of the interview guide. This structure allowed us to explore the perspectives of key stakeholders and law enforcement agency officials in a systematic manner while adapting to the flow of the conversation.

Table 6.2: Sample Interview Questions

Phase	**Sample Question**
Consent and Privacy	Could we please get your consent signature for this session so that we can record it and use it later in our further research?
Flexible Duration	Will you give your 25–30 minutes for our interview? If we need more time, will you provide your valuable time?
Initial Awareness	What do you think about the current reporting platform of Bangladesh? Is it effective or not? What improvements can you suggest?
Deeper Probing	Can you describe a short story related to cybercrime handling? Will you be willing to elaborate for us?
Conclusion and Feedback	Will you give us some suggestions for improving the cybercrime-reporting platform from a Bangladesh perspective?

6.4 Findings and Thematic Analysis

The current section will show the main results of the interviews carried out with the stakeholders within the cybercrime-reporting system in Bangladesh. The analysis will be done in terms of some of the salient themes that were identified in the course of the interviews. These themes reflect the system, operational and usability

difficulties which are already existing, impairing the effectiveness of the reporting process. The discussion will provide a general overview of the findings, after which the discussion will delve into the areas of disparities in access and awareness, limitations of platforms, siloed data ecosystems, identity verification challenges, and gaps in resources among other crucial challenges which were found to undermine the success of cybercrime reporting in Bangladesh. We also give practical suggestions on how to improve the existing systems and to deal with these challenges. This thematic analysis will help us to identify the underlying causes of inefficiencies and provide practical recommendations to improve the experiences of citizens and law enforcement.

6.4.1 General Findings

Overall, the interviews indicate that the current state of intake pipeline and the back-office environment is fragile and split, making the cybercrime reporting painfully slow and unpredictable to both citizens and officers. Verification is not reliable, cases are treated through various handoffs, with evidence potentially lost, and data is isolated among agencies. Sites offer minimal directions or visibility, and individuals are unable to make corrections on their submissions, provide evidence, or monitor the status, which results in redundancy and dismay. The collaboration with social platforms and banks is sporadic and staffing and IT-training gaps push the capacity. Language barriers, connectivity barriers, and digital illiteracy disproportionately impact rural users and a substantial proportion of women. VPNs and disposable numbers contribute to the further complications of common harms (e.g., Facebook bullying, mobile-money fraud, blackmail). The interviews thus indicate workable redresses: strong, twenty-four-hour ID checks; direct digital consumption with lossless evidence management; a centralized and role-based case system with intelligent triage; explicit status and citizen follow-ups/edits; and formal and safe information-sharing with platforms and monetary institutions.

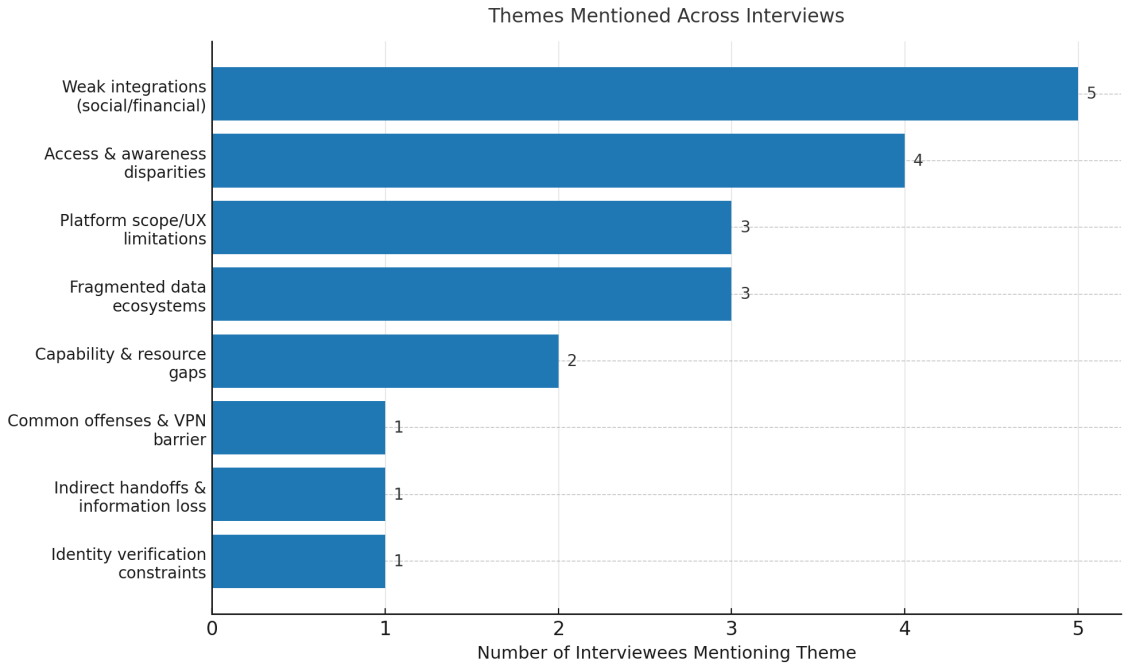

Figure 6.1: Themes mentioned across interviews (N=5). Bars show how many interviewees raised each theme at least once.

Figure 6.1 shows that *weak integrations with social and financial platforms* was mentioned by all interviewees, making it the most universal constraint. *Access and awareness disparities* was the next most common theme, followed by *platform scope/UX limitations* and *fragmented data ecosystems*. Fewer—but still important—mentions concerned *capability and resource gaps*, *indirect handoffs and information loss*, *identity-verification constraints*, and *common offenses with VPN barriers*. Read together, the distribution indicates broad agreement on cross-agency coordination and citizen access as the most pressing issues, with technical UX and workflow weaknesses close behind.

Overall, the interviews converge on three root causes of delay and low trust: brittle verification and routing at intake, siloed data and weak external cooperation, and interfaces that neither guide citizens nor support efficient triage. Addressing these requires a dual focus on user experience and operations: (i) dependable verification; (ii) streamlined, auditable submission that preserves evidence; (iii) a centralized, role-based case system with automated prioritization; (iv) transparent status with citizen-side edits and follow-ups; (v) targeted training and resourcing; and (vi) formal, secure data-sharing with social media and financial institutions. These priorities guide the requirements and design decisions formulated in the work following.

6.4.2 Access and Awareness Disparities

Official at the National Security Intelligence (NSI) observed that there is a general unawareness among people concerning online sites where cybercrime cases can be reported. There is the 999 hotline which can be utilized but only provides partial assistance with cyber-specific complaints. In addition, the DMP (Dhaka Metropolitan Police) SI revealed that there was no information sharing between the relevant

sectors, and the problem was further aggravated by a shortage of the personnel. Another challenge that is faced by rural residents, especially women, is the use of various languages and lack of internet connectivity. The necessity to possess a regional data storage facility, instill trust in the stakeholders, raise more awareness programs to more people, and sealing communication barriers between service providers and service seekers were identified.

6.4.3 Platform Scope and UX Limitations

The BFIU officials mentioned that the lack of user controls and interactivity in existing systems as a critical limiting factor. System centralization, increased publicity activities, data-sharing agreements among financial institutions, and frequent system audits were proposed as effective remedies.

6.4.4 Fragmented Data Ecosystems and Cross-Agency Coordination

The involvement of banks in dealing with monetary cybercrime cases complicates investigations, whereas an official from the Bangladesh Financial Intelligence Unit (BFIU) proposed local cloud storage as a possible solution to provide better data protection. In addition, the fragmentation of the financial institutions complicates the process of administering complaints as well as exchange of information. However, a representative from the DMP Cybercrime Unit noted that large financial institutions tend to resist integrating external platforms, which makes fraud investigations more difficult.

6.4.5 Identity Verification and Authentication Constraints

It was noted that an official from the DMP Cybercrime Unit found that police face trust issues with the Online GD platform, as it is difficult to verify whether a user's complaint is real or fake. The NID Server and the Police Server are not properly connected, which complicates the verification process. By using the CDMA server, the police could search a person's NID and determine if it is genuine or fake. However, the official mentioned that the CDMA server is no longer easily accessible to the police. Currently, the police can only search 20 NIDs per day through the CDMA server, significantly limiting their capacity. Though the CDMA server is a powerful tool of checking the NIDs, the official indicated that the policymakers have not given complete access to this server, which has also hampered the adequate verification of identity. Furthermore, the official stated that Online GD App by BD Police only accepts the complaints connected with the lost items at the moment, e.g., a lost phone. The complaint systems available online do not have a proper system of user verification and this is why face to face complaints are favored. The Online GD platform does not support proper questioning and inquiries, particularly when it comes to complaints that are more complex than those of lost items. Consequently, the official clarified that the police disapproves online GDs on most categories of complaints, only taking the ones that concern lost items, where main enquiries are not required.

6.4.6 Capability and Resource Gaps

One of the representatives of the DMP Cybercrime Unit mentioned the problematic situation because of the absence of data-sharing agreements with social media platforms, as it is hard to cooperate and identify fraudsters. The proposed changes were IT training to law enforcement, better interface to the platform, tougher punishments on false reports, and enhanced collaboration with social media providers. However, there are several impediments including the inaccessibility of platforms, absence of resources and disproportionality of officers compared to the general population.

6.4.7 Common Offenses and VPN/Anonymity Barriers

According to an official of the DMP Cybercrime Unit, Facebook bullying, mobile fraud, and blackmailing were some of the other common cybercrimes where victims were aged between 20 and 30 years. Additionally, the utilization of VPNs by the criminals hinders the investigation process, which presupposes providing more technical resources and cooperation with the technological companies to share the information.

6.4.8 Recommendations and Improvements

The outcomes of the interview indicate that several recommendations can be given on how the system of cybercrime-reporting in Bangladesh can be enhanced. First of all, one of the representatives of the NSI pointed out that the awareness campaigns should be given a due urgency, to make people (especially the rural population and women) more aware of the available reporting channels. These campaigns should capitalize on mass media, social networks, and outreach to the community so as to educate the citizens about their rights and available reporting systems. It is also important to improve the technological infrastructure. According to a Sub-Inspector of the DMP, the system must support a high degree of authentication of any form of verification including NID and birth certificates to enhance confidence as well as cut down on abuse. As one of the representatives of the BFIU mentioned, the ability to process real-time data and store it on the local level through dynamic and centralized platforms would offer substantial improvement in the efficiency of the operations. It is also characterized by a significant need to increase IT training on all levels of law-enforcement agencies. Digital literacy and other relevant technical knowledge provided to officers will improve their qualifications to handle cybercrime cases and report systems. One of the BFIU representatives also added that resource allocation must also be given priority to include system upgrade, platform improvement, and infrastructure development. It is obligatory to cooperate with other stakeholders such as social media organizations and even financial institutions in order to support the investigations and increase the information sharing. A representative of the DMP Cybercrime Unit advised that appropriate policies and data-sharing agreements ought to be established to help in coordination and proper handling of cybercrime cases. Decentralisation of the cybercrime management is also another important recommendation. According to the DMP Cybercrime Unit official, there should be a policy that should allow the local police stations to act on cases of cybercrime so that a central working agency does not have to bear the burden and should

be able to report cases more easily. Finally, there are punitive actions to address false reporting that are significant to the integrity of systems. A representative of the DMP Cybercrime Unit stressed that proper monitoring systems and penalties against making fake complaints will help instill confidence in people and prevent misuse. All these recommendations are likely to enable a more effective, convenient, and dependable system of cybercrime reporting in Bangladesh.

6.4.9 Systemic Challenges

The interviews also unveiled several gravity issues that affect the functionality and performance of cybercrime-reporting sites in Bangladesh. A NSI official emphasized that the lack of awareness in the population, especially those living in rural areas and women, is one of the issues due to the absence of outreach efforts and user guidelines. The official also indicated that low internet access, language differences, and insufficient digital literacy also discourage vulnerable groups to report cyber incidents. Banks, law enforcement and service providers were also found to be operationalised in such a way that creates delays and inefficiencies in the processing of complaints. According to a representative of the DMP Cybercrime Unit, the trust in existing online services is low because of the poor user verification and difficulty in accessing the NID authentication systems; this forces police to still use face to face reports. There are technological loopholes between reporting systems. Existing locations lack user-friendliness, cannot authenticate in real-time, lack secure data processing; cybercriminals can utilize VPNs, spoofed SIM cards and unregistered mobile accounts to escape detection. One official at the DMP Cybercrime Unit pointed out that the lack of qualified personnel, the lack of sufficient ratio to the police and the lack of IT capability in law-enforcement departments also contributes to the inefficiency of the system. Formal agreements with social media services and opposition of financial services restrict cooperation since government agencies struggle to get information about criminals. Furthermore, complaints tend to pass through a number of levels such as local police and cybercrime departments, which results in loss of information and slow response. A representative of the DMP Cybercrime Unit added that the current system of digital infrastructure is able to perform only superficial complaints, like the loss of an object, and is not thoroughly verified, which is a negative indicator of trust in the online platform. Such limitations and the increased percentage of cyberbullying and financial frauds demonstrate the urgent need to have a single, accessible, and trusted framework of cybercrime reporting which will prioritize its convenience and inclusiveness as a fundamental principle.

Chapter 7

Data Analysis and Synthesis

This chapter analyzes the data based on three fundamental approaches: user testing involving 40 participants, heuristic evaluation based on five HCI experts, and interviews with five key officials. These are to be triangulated to identify system-wide usability problems within the cybercrime reporting systems in Bangladesh. Through the comparison of the rate of task failures, user frustrations, expert severity rating, and insight on the sides of stakeholders, the chapter gives a comprehensive perspective of why these digital services fail to satisfy user needs and thus people use conventional face-to-face reporting. This discussion initially shows the results of user tests, then superimposes with the evaluations by experts, and finally, an analysis of interviews is provided.

7.1 User Testing Data Analysis

The user testing with 40 participants across different professional and technical domains clearly showed that there were extreme usability issues in-particular CID, DSA, BTRC Websites and the Online GD mobile app. Anecdotal evidence shows compelling arguments for those who encounter these websites.

7.1.1 Task Success and failure Measures

The clearest signal of system failure, however, was the woeful performance at task completion. As Table 7.1 shows, the central activity of reporting a complaint is found on these most websites too tough to do. Although the CID website was a reporting system, only approximately one in ten of the cases were followed up on. Most critically, the DSA and BTRC websites all had zero task completion rate as there was no incident of existence of an accessible on-line cybercrime reporting form by any of the 40 users. The Online GD app did no better, barely managing a 15% estimated completion rate, significantly impaired by technical glitches such as the app crashing when attempting to submit.

The respective failure rates for the most important points of failure were additionally presented on platforms, as illustrated in (Figure 7.1) and so on. The Y-axis does not show the category of failed call attempt.The high incidence of “Form Not Found” across the DSA and BTRC sites, as well as “Disorientation” and “Back Button Failure” on the CID site clearly depicts how these failures are classified in

Table 7.1: User Testing - Task Completion Metrics and Failure Rates by Platform

Platform	Task Completion Rate (Estimated)	Key Task Failure Metrics
CID Website	$< 10\%$	• 38/40 (95%) users were disoriented. • 29/40 (72.5%) could not find the complaint form initially. • 40/40 (100%) received no confirmation after submission.
DSA Website	0%	• 40/40 (100%) users could not find an online complaint form. • 5/7 (71.4%) helpline call attempts failed or had excessive wait times.
BTRC Website	0%	• 40/40 (100%) users found no online complaint form for cybercrime.
Online GD App	$\sim$15%	• App crashes during form submission. • Authentication failures (Face-scan, OTP delays). • 100% received no submission confirmation or tracking.

terms of their contentlessness being expressed. This is a trust-breaking failure to fail on "no confirm" and it fails across the board everywhere we had a form.

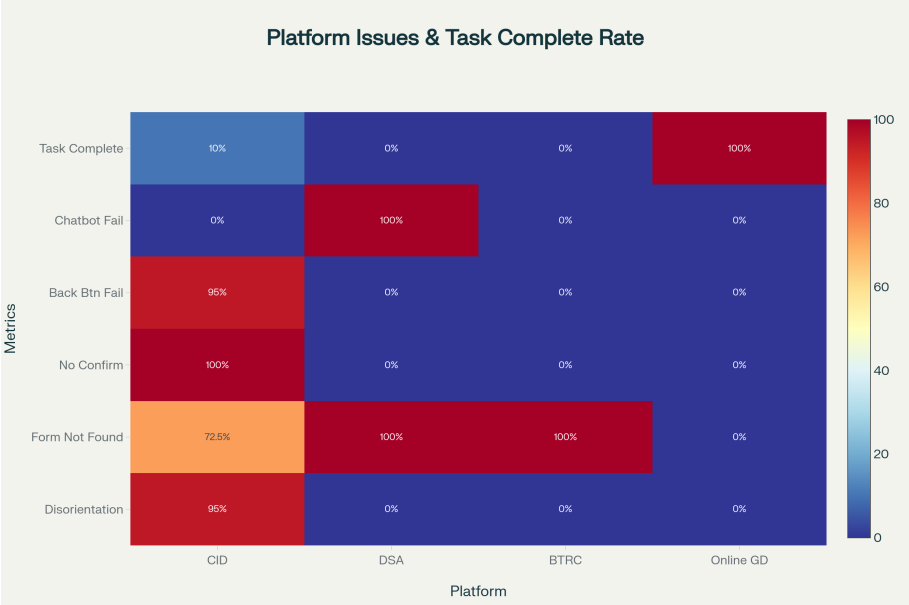

Figure 7.1: Heatmap of Platform Issues and Task Complete Rate

7.1.2 Thematic Synthesis of User-Reported Platforms

A systemic classification of user feedback further identified the dominant problem themes and their significant influence on the usability and perceived credibility. The following are summarized in Table 7.2.

The connection between the frequency of these problems and their importance to the UX is explored more in (Figure 7.2) Navigation, Design, and Forms issues were not only common but of high to critical direct impact resulting in task abandonment.

Table 7.2: Synthesis of User-Reported Problems and Prevalence

Problem Category	**Specific Issue**	**% of Users Affected (n=40)**	**Impact on User & System**
Navigation & Findability	Cluttered design; unable to find complaint form.	95% – 100%	Users become disoriented and abandon tasks; prevents access to core service.
Design & Layout	Outdated, non-mobile-friendly, overcrowded pages.	72.5% – 100%	Creates a poor first impression; hinders efficiency and accessibility.
Forms & Submission	Forms are complex, lengthy, and contain errors.	77.5%	Increases user effort and likelihood of errors during critical reporting.
Feedback & Trust	No confirmation, tracking ID, or status updates.	32.5% (explicitly), but impacts all	**Critical failure:** Erodes credibility and trust; users feel their report is lost.
System Reliability	Broken links, non-functional search, helpline busy, app crashes.	Varies (e.g., Search ER: 37.8%)	Causes frustration and task failure; reinforces perception of a broken system.
Security & Verification	Lack of user verification (e.g., NID, OTP).	16% (explicitly)	Undermines trust for sharing sensitive data; users fear for their security.

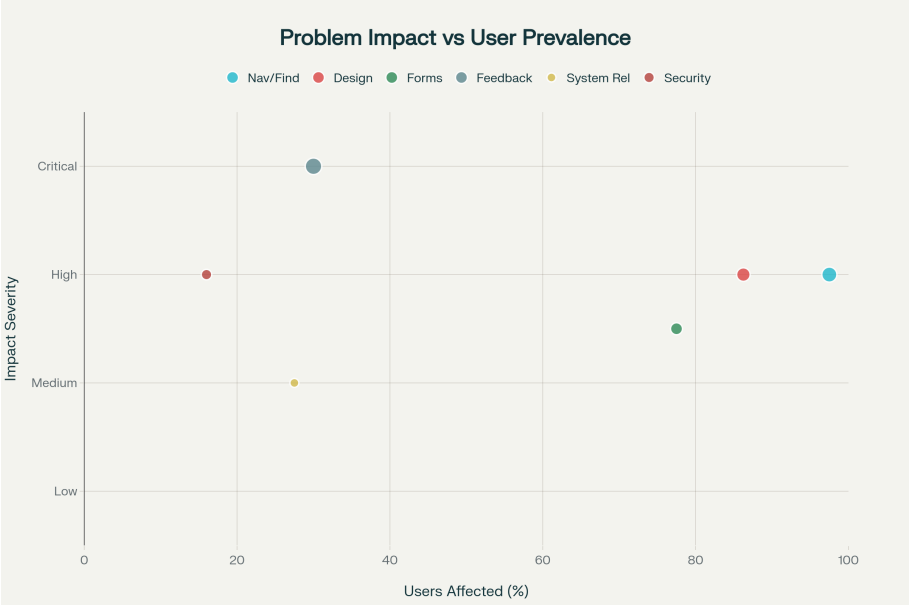

Figure 7.2: Bubble Chart of Problem Impact vs. User Prevalence

These metrics were highly framed by the qualitative data of the think-aloud protocol and post-test interviews. The users reported feeling "confused" and that they found the site "difficult to navigate".

7.2 Heuristic Evaluation Data Analysis

The heuristic evaluation was used as a diagnostic tool to explain user failures exposing the fact that they had broken well-established principles of usability. The expert judgment (Table 7.3) scored their level from 0 to 4.

Table 7.3: Heuristic and Usability by Platform: Usability Issues Severity Ratings

Nielsen's Usability Heuristic	**CID**	**BTRC**	**DSA**	**Online GD**	**Key Issues Identified (Summary)**
Visibility of System Status	2	4	2	1	Users do not see confirmation messages and cannot track progress.
Match b/w System & Real World	2	2	2	3	Specialist terms and language that normal users find difficult.
User Control & Freedom	1	2	1	2	Few ways to reverse actions; no feature to edit or withdraw submissions.
Consistency & Standards	2	2	3	2	Inconsistent terminology and navigation across screens.
Error Prevention	2	1	3	2	No adequate error-prevention mechanisms; allows invalid form submission.
Recognition Rather Than Recall	2	2	3	2	Users must remember too much; lack of autofill or memory aids.
Flexibility & Efficiency of Use	3	4	4	3	Repetitive data entry; no templates, advanced search, or filters.
Aesthetic & Minimalist Design	1	3	3	1	Cluttered layouts with excessive content; difficult to navigate.
Help Users Recover from Errors	1	3	1	2	Unclear error messages; no correction option or troubleshooting support.
Help & Documentation	3	3	2	2	Lacks extensive support resources (FAQs, user guides, instructions).
Cumulative Severity Score	**19**	**26**	**24**	**20**	BTRC has the highest total severity, indicating the most severe usability challenges.

The data table reveals that BTRC accumulated the highest cumulative severity score (26), branding it the platform with the most catastrophic usability problems, notably in "Visibility of System Status" (rated 4) and "Flexibility Efficiency of Use" (rated 4). Online GD app, although having lower scores in certain aspects, had a big breach in its match between system and real world (rated 3) as the small range of the lost and found items was not relevant to the real life of the users who need complex cybercrimes reported.(Figure 7.3)

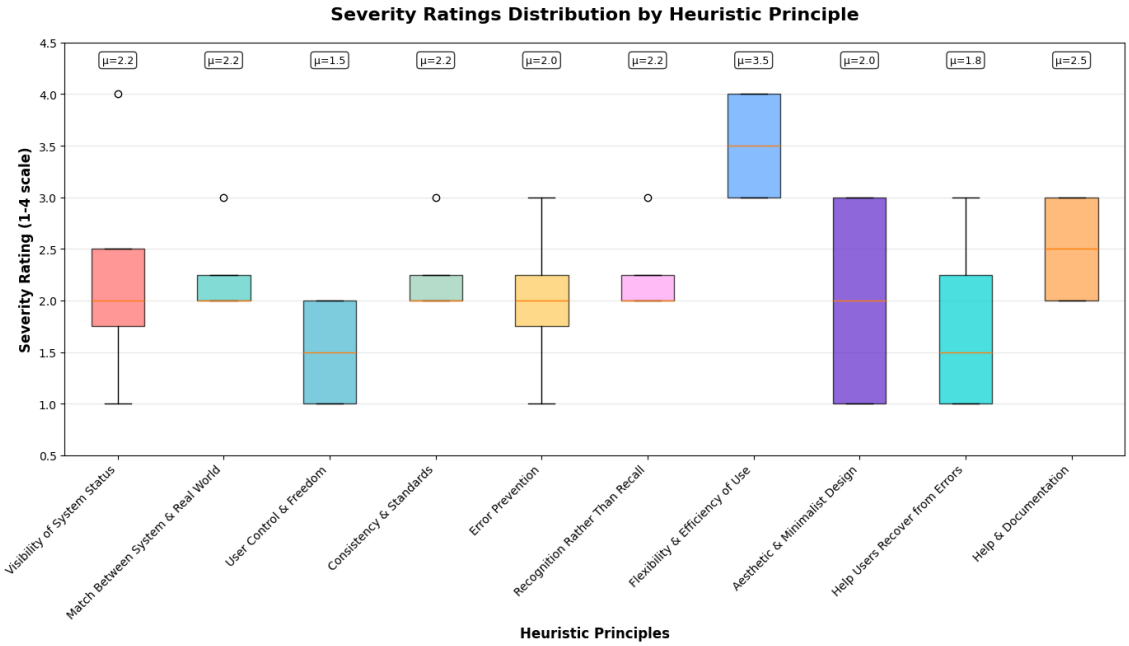

Figure 7.3: Boxchart of Heuristic Severity Ratings

7.3 Development of Qualitative Interview Perspectives

The interviews conducted with the NSI, CID, BFIU, and DMP Cybercrime Unit officials provided a significant operational background to the above-described usability failures. These are not individual user interface design issues but indicators of more profound organizational and procedural issues.

One of the key discoveries was the disjointed and poorly connected reporting system. According to the officials, the complaints are constantly registered in the police and cybercrime departments, leading to information losses and delays. This is similar to user test findings of confusion and disorientation in the platforms. Weak infrastructure was also confirmed during interviews, which includes poor user authentication due to unreliable NID verification on the CDMA server.

Major barriers were found to be low public awareness, and digital literacy among rural users and women. This corroborates the heuristic discovery of bad match between system and real world since the platforms presuppose digital skills that most users do not have. Interviews also disclosed that the financial institutions and social media sites are not keen on giving data which might impede investigations and create more suspicion among the users on the need to share sensitive information online.

7.4 Triangulation of Results and Cross-Cutting Themes

Combining data across all three sources results in a number of strong cross-checks that mutually support and validate each other:

The Trust Void: Quantitative user testing shows that 100% of users on major platforms got no feedback for the submit. In the heuristic evaluation, this was termed as failure of a "visible system status". The interviews confirmed this: The limited verification and tracking makes it so that officers have to depend on in-person, with the information loop feeding on itself: Digital systems aren't trusted if they're not trustworthy.

The 'Findability' Crisis: The 0% figure for task completion on DSA and BTRC in this specific use case – that of users not being able to find the complaint form they are looking for – is a direct result of Heuristic Evaluation failures ("Aesthetic and Minimalist Design" (Cluttered layout) and "Match Between System and Real World"(The sites don't actually work as reporting sites users expect)). To make the findability issue more difficult, interviews have reported that not many people are aware of these platforms in the first place.

Systemic, Not Superficial Failures: These problems are in deep rooted on the flaws of the platform design (heuristic evaluation), verified by the failures of the users (user testing), and supported by the gaps in operation (interviews). Poor "Error Prevention" and "User Control and Freedom", which is manifested through strict forms and lack of navigation, is pointed out by professionals as problematic, which officials admitted to be the shortcoming of the design.

Cumulatively, the discussion indicates that the monitoring processes of cybercrimes in Bangladesh lack critical problems of usability at both interface and operations. They are not user-friendly and do not entail trust-building qualities and this makes users to forget about digital alternatives and go back to conventional, manual ways of reporting.

Chapter 8

Proposed website

In this section will introduce a new system for a cybercrime reporting platform. The proposed design platform will be user-friendly, secure, and accessible to the general public of Bangladesh. Spring Boot, PostgreSQL, React.js, and Docker achieve high availability and scalability. Its features include secure login, a dashboard, a chatbot, filing of complaints with attachments, and real-time tracking of reports. Other features, such as fraud awareness, news, and feedback, enable users to trust and participate in the system, providing an efficient and user-friendly reporting experience.

8.1 Design Rationale Based on Data

The design choices made for the proposed cybercrime reporting tool are driven by data analysis of user interviews, heuristic evaluations, and contextual inquiries. The findings of this study reveal some common usability problems existing in both systems, such as convoluted navigation paths, insufficient feedback for users, and a lack of functionality for users to customize. One of the frequently reported issues was a clear and accessible user interface for a wide users with varying levels of digital literacy in Bangladesh.

Security has become of paramount importance, and a trade-off between rigid protective means and user convenience must be achieved. To mitigate this, we tailor protection to the user's context and identify risk levels, providing strong protection with minimal overhead on users. Furthermore, it was emphasized that the timely update of actual running conditions and successful/failed reporting confirmation is critical to maintaining user trust in the reporting system.

Additional design improvements were informed by user feedback, indicating help with structured complaint submission and step-by-step instructions, as well as processes that simplified the steps to reduce cognitive load. These data-driven understandings point to the importance of developing a system that balances engineering sophistication with an excellent user experience. With usability, security, and inclusivity considerations in place, the platform is designed to improve significantly user engagement, trust, and effectiveness under the Bangladesh socio-technical (cybercrime) environment.

8.2 Tools and Technologies Used

In this section, we will discuss the elaborate use of modern frameworks, programming languages , and deployment tools to ensure usability for our proposed system.

Spring Boot (Backend Framework): The Spring Boot framework has been utilized to implement the backend system, a Java best practice framework. The goal is to simplify the creation of a production-ready application with minimal configuration. It supports REST API development with dependency injection and modular microservices. [53]

PostgreSQL (Database Management System): PostgreSQL was chosen as the primary relational database management system due to its robustness in terms of ACID compliance and its ability to handle complex queries and transactions efficiently. [54]

Docker and Docker Compose (Containerization): Docker and Docker Compose are used to simplify environment management and deployment. It allows for containerization of the database and backend, ensuring consistency between development and production environments. [55]

React.js (Frontend Framework): Our frontend is developed using React.js and JavaScript libraries. It provides the facility to create components in the user interface with reusable components and provides optimized virtual DOM rendering. [56]

Git and Vercel: Git was employed for better distribution of version control. It also allows effective codebase management and collaborative development. The frontend was deployed using Vercel. Verce is cloud base platform for Forontend and react.

Testing Tools: As a developer, we used JUnit and Mockito for user testing. For frontend validation we used React/Just testing library.

8.3 Key Features of the System

The system ensures that it possesses key features, making it both user-centric and technically superior. In this section, the key features will be described. The following features highlight the main contributions:

Security login and registration: We implement a token-based authentication process and Spring Security for secure login, registration, and role-based access. After registration, the admin will approve and authenticate the user. User can also reset the password of their account. (Figure 8.1, 8.2, 8.3, 8.4)

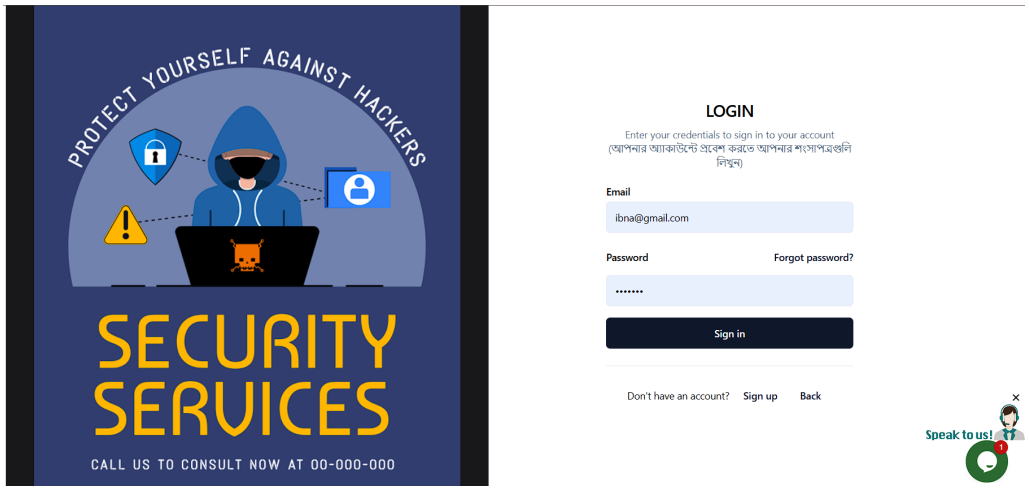

Figure 8.1: Login page

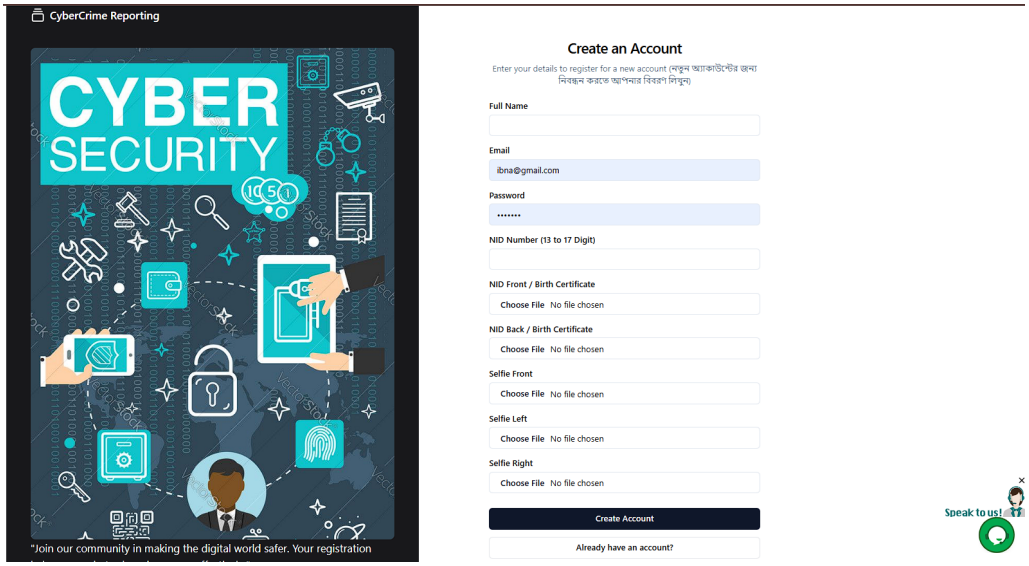

Figure 8.2: Registration page

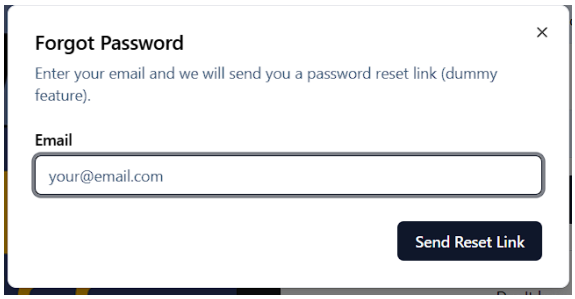

Figure 8.3: Forget Password

Figure 8.4: Admin approval

User-friendly UI Design: To enhance user experience, we design a more intuitive UI. In our UI, we kept each page simple and easy to navigate, so that users can understand the website and the key terms. (Figure 8.5, 8.6, 8.7, 8.8)

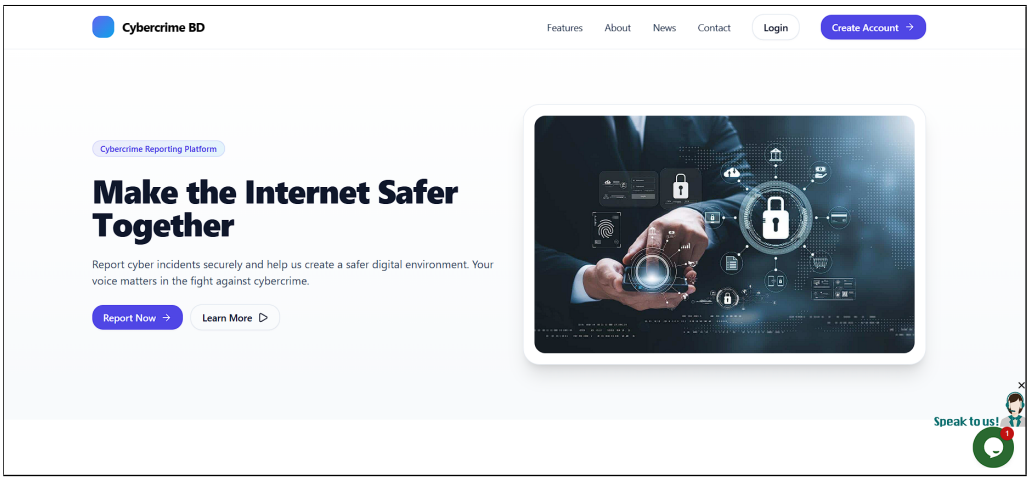

Figure 8.5: Landing page

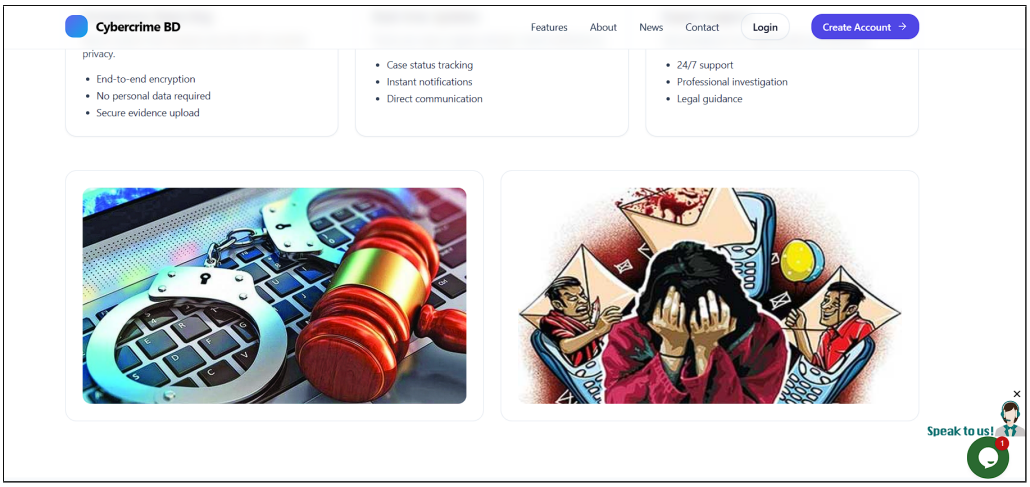

Figure 8.6: Landing page

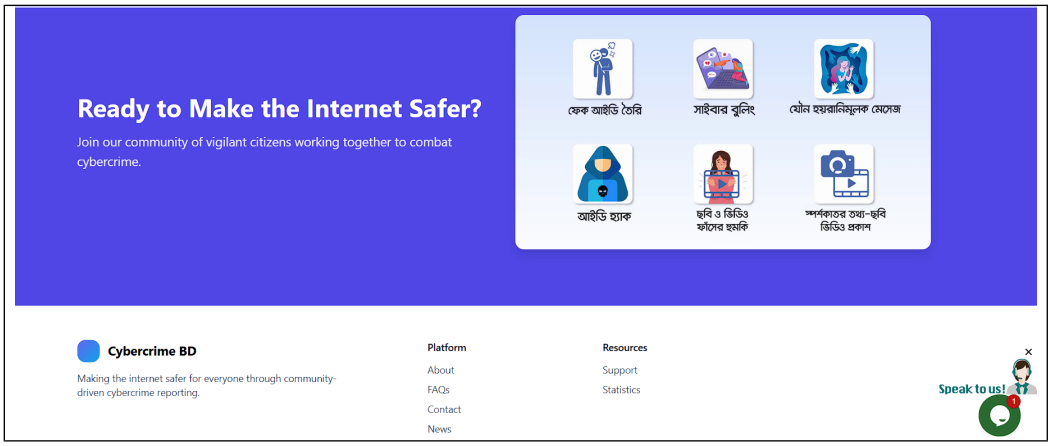

Figure 8.7: Landing page

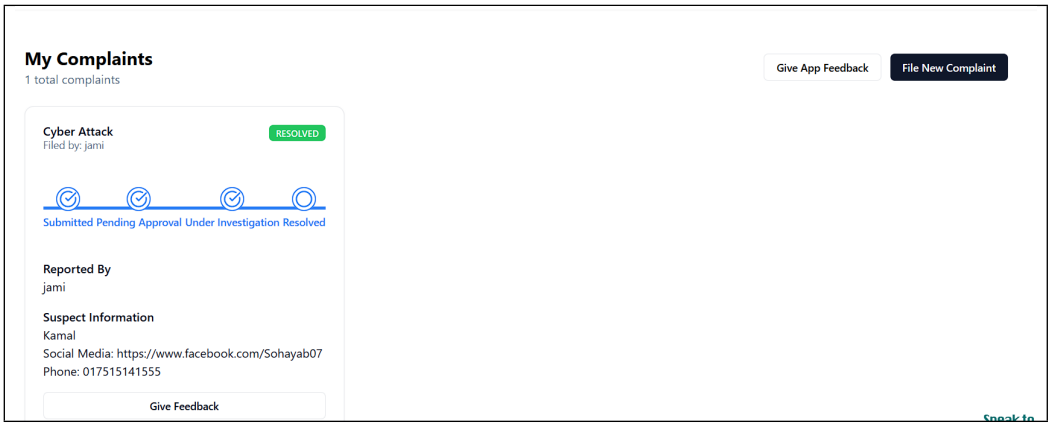

Figure 8.8: User dashboard page

Chatbot: We have implemented a real-time communication system, which is a chatbot. Users can communicate directly with the admin through this chatbot. They can share feedback, ask questions, and report issues. Users may also attach

photos and documents in the chat. (Figure 8.9)

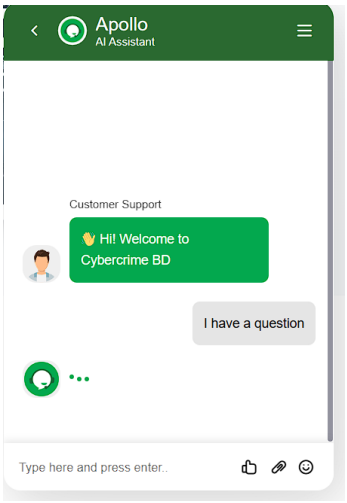

Figure 8.9: Chatbot

Complaint Process: The user can select the department corresponding to their issue. The complaint will be assigned to that department, and then the selective department admin will process the complaint. Then, the author will address the issue selectively. Additionally, users can add suspect information and an evidence attachment file, which can include a screenshot or any other relevant file. Also, users can edit their complaint file after submission. (Figure 8.10, Figure 8.11, Figure 8.12)

Figure 8.10: Complaint Form

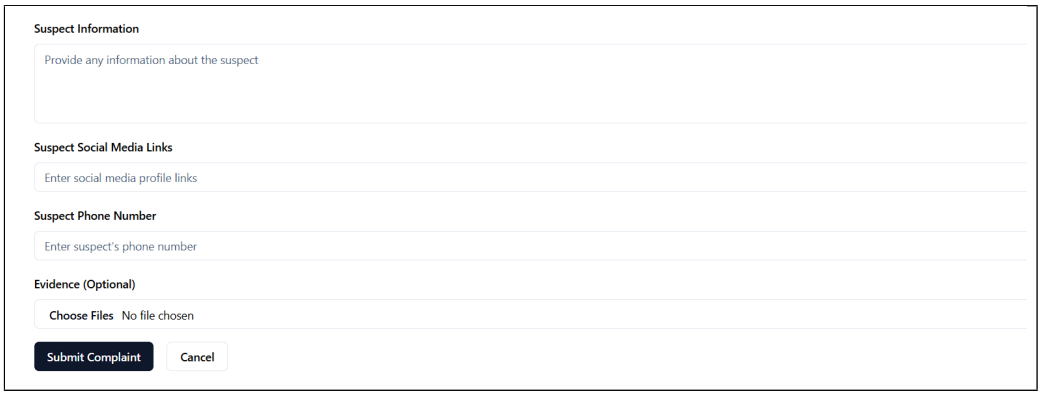

Figure 8.11: Complaint Form

Figure 8.12: Complaint Edit

Report tracking: After filing a complaint, users will be able to view the current stage of their report and the next stage it is transitioning to through a tracking system. Users will be able to see the stage their complaint is at and where it is being processed. (Figure 8.13)

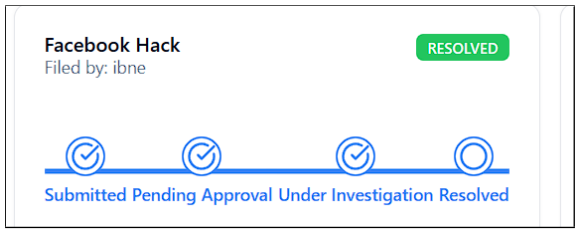

Figure 8.13: Report tracking

Guidance Section: Sections such as 'About' and 'Types of Fraud' will help users better understand our website, and they can also learn about various types of fraud. The news section will help users discover the variety of news and gain knowledge. (Figure 8.14,Figure 8.15,Figure 8.16,Figure 8.17,Figure 8.18,Figure 8.19,Figure 8.20)

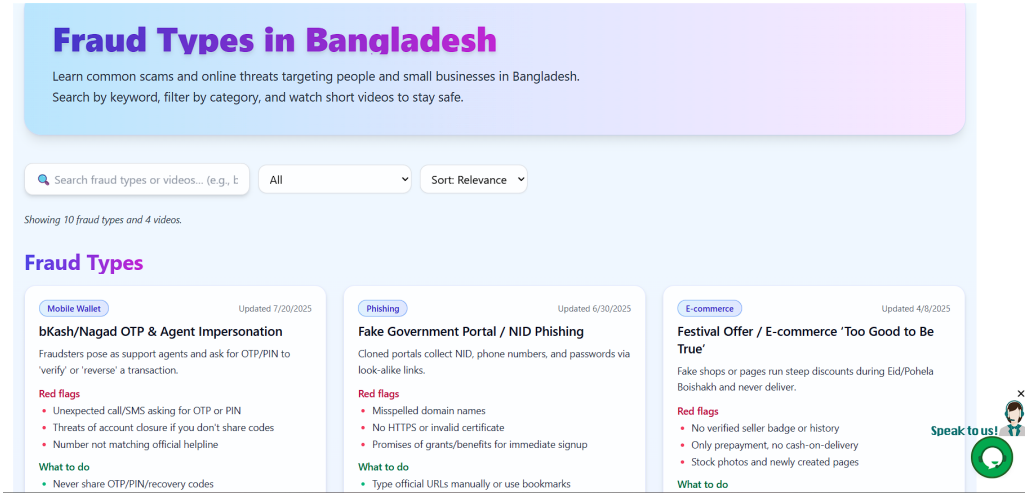

Figure 8.14: Fraud type

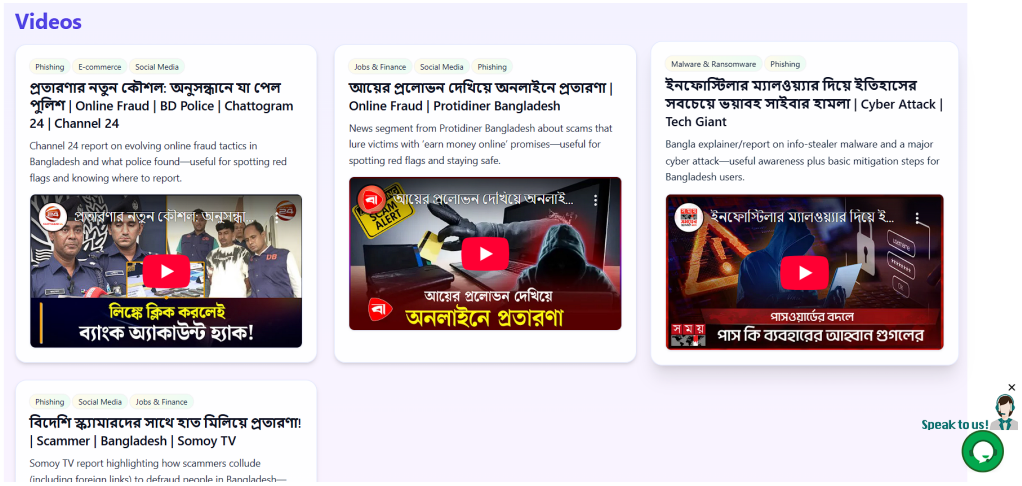

Figure 8.15: Fraud type

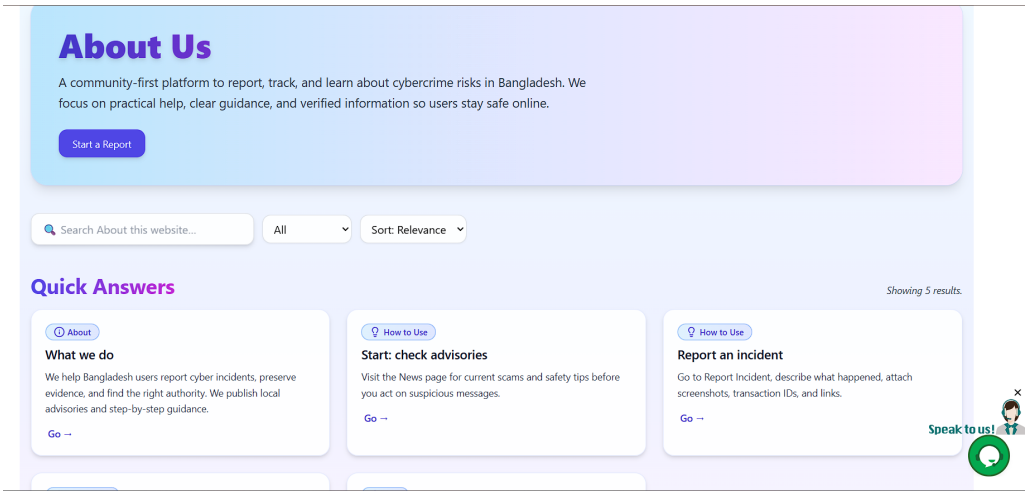

Figure 8.16: About Us

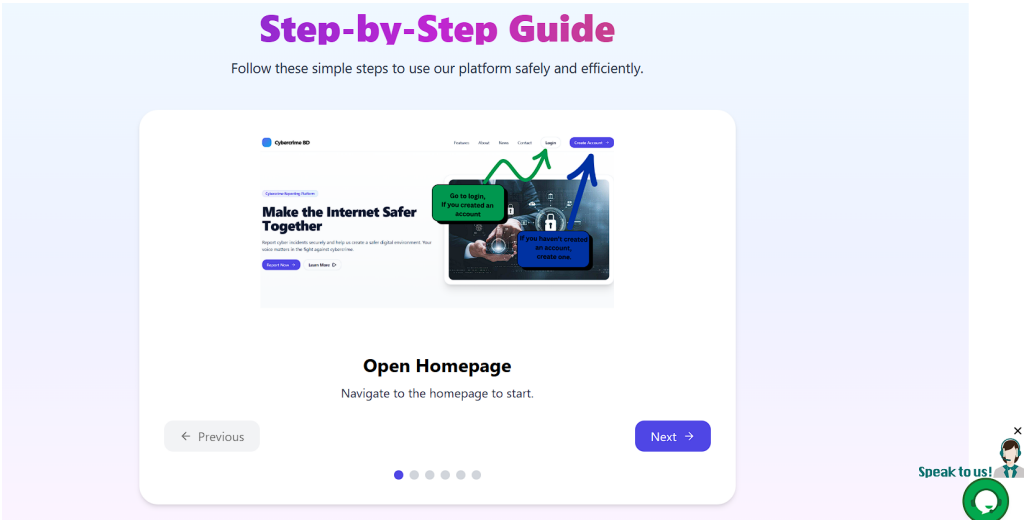

Figure 8.17: Step by Step Guide

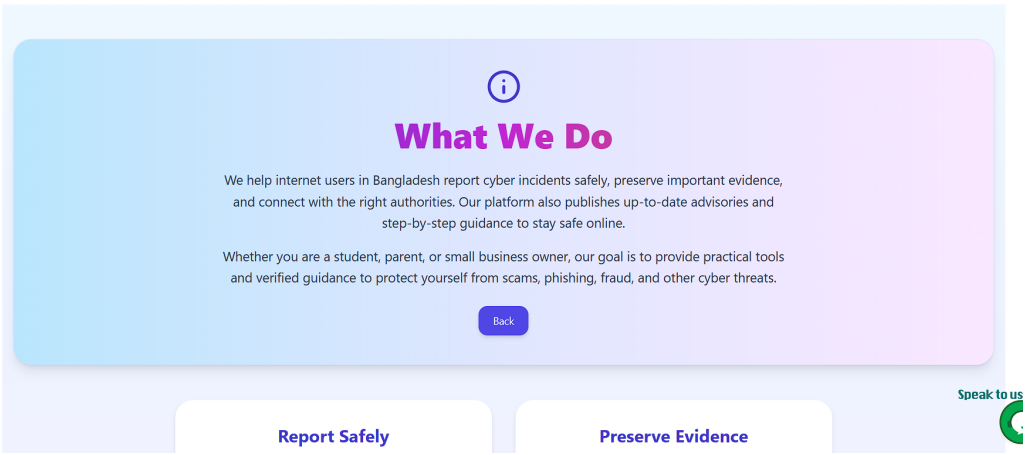

Figure 8.18: About Us

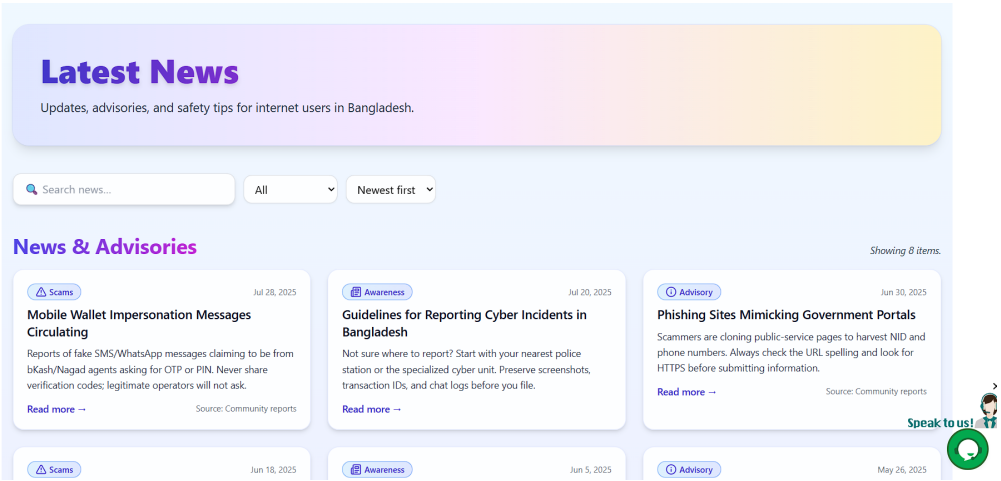

Figure 8.19: News

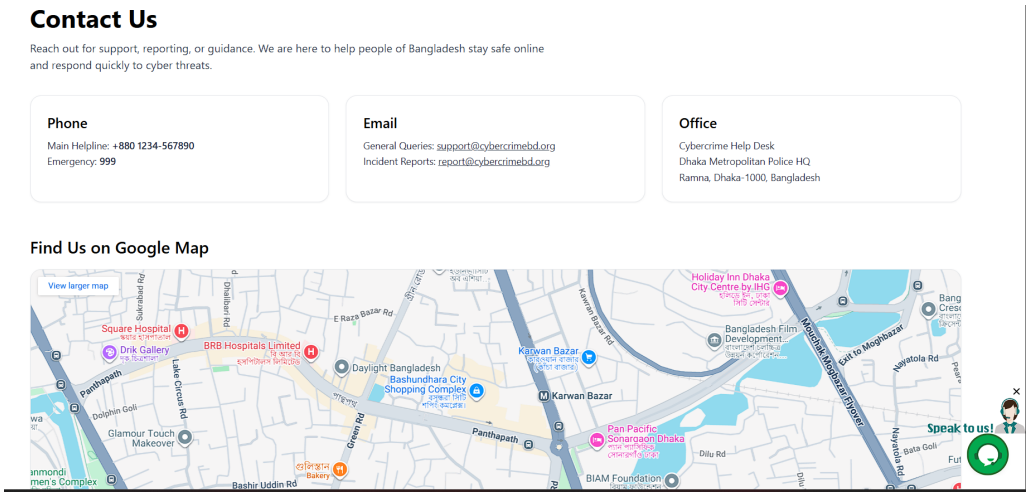

Figure 8.20: Contact

Search: In every section, users will find a search feature that helps them find their respective queries. (Figure 8.21)

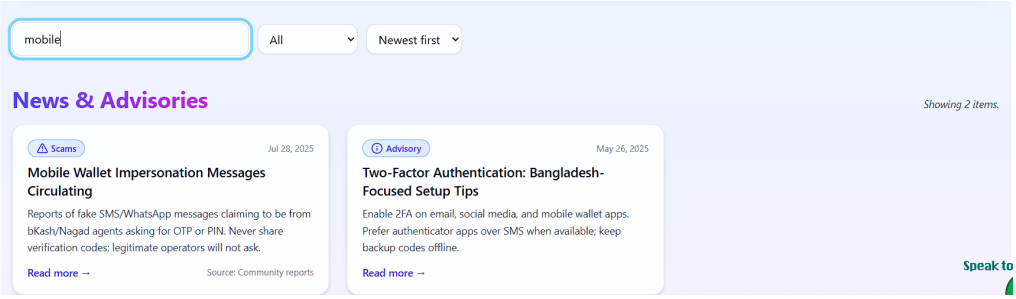

Figure 8.21: Search

Feedback: After submitting a complaint, users can provide initial feedback. Additionally, users can offer feedback about the entire website using separate buttons, which will allow them to submit their queries and opinions to the author at both levels. (Figure 8.22, Figure 8.23)

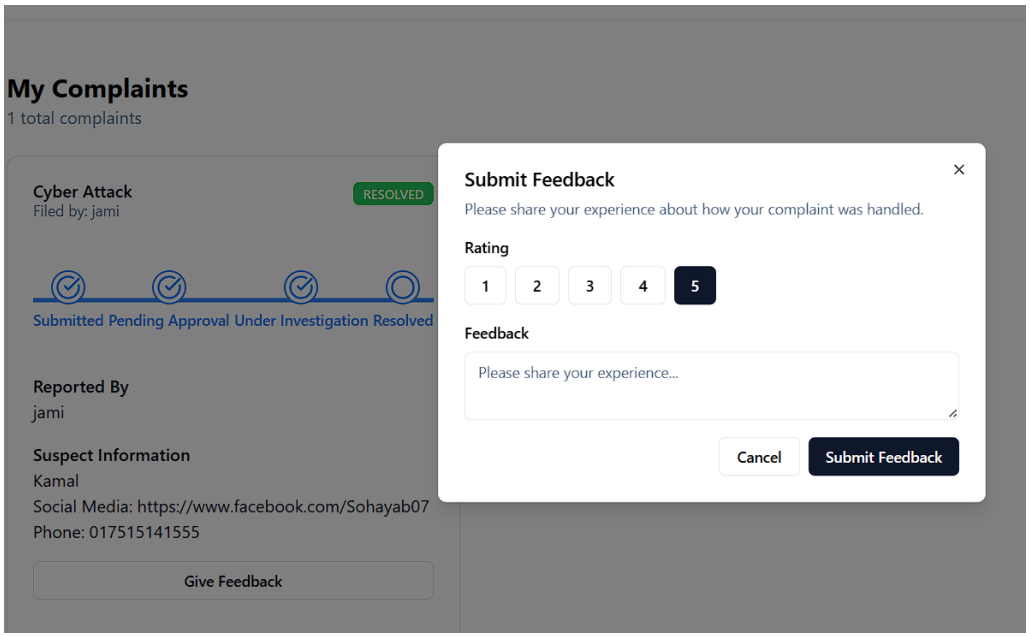

Figure 8.22: Complaint Feedback

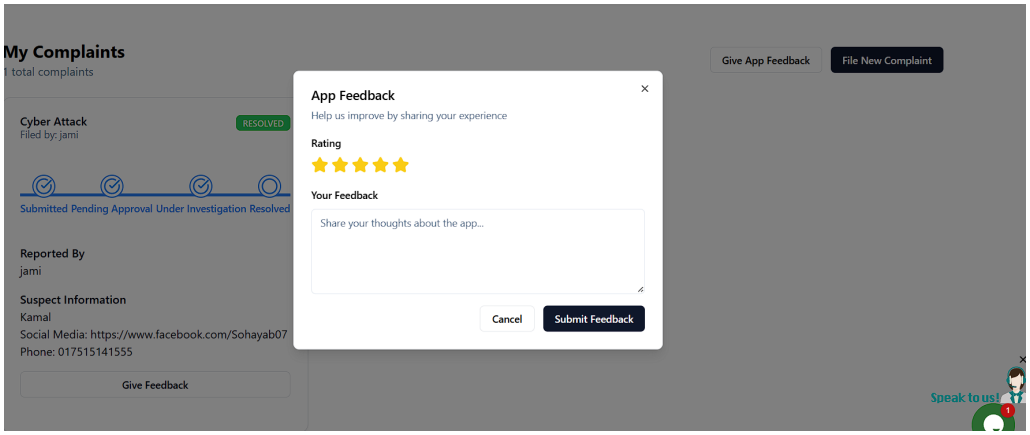

Figure 8.23: Website feedback

Chapter 9

Usability Evaluation of the Proposed Website

The primary objective of this chapter is to describe the testing of the proposed system, which has been implemented and evaluated in a structured user testing environment. In the first phase of our research, we examined and tested several Bangladeshi government cybercrime reporting websites, including Criminal Investigation Department (CID), Bangladesh Telecommunication Regulatory Commission (BTRC), and the Digital Security Agency (DSA),and evaluated their usability effectiveness. Following the constraints and users' feedback on these platforms, a new website was designed and implemented to provide an alternative solution for enhancing the online submission of cybercrime reports. This chapter presents the results of the user study on the proposed website, aiming to gain insight into how users interact with it. It also examines the feasibility of such a system for citizens to use, should a government instance deploy it. More specifically, the usability evaluation aims to assess whether the website is an easy-to-use tool for users and whether they can clearly understand how to perform tasks and report on them. Are users also willing to use a website like this if it were deployed by the government as an official site to handle cybercrime reports in Bangladesh? Additionally, to determine whether participants would use such a site to report instances of cybercrime in real life.

In this system evaluation process, a total of 40 participants took part, aged between 23 and 36. Moderated user testing rules followed the evaluation process. Since the platform is a proposed and not connected to real government systems, participants interacted with simulated data while carrying out the assigned tasks. Throughout the process, the researchers closely observed the participants' actions, noted their difficulties, and collected both quantitative and qualitative feedback. The results of this evaluation inform the usability of such a designed system and its potential to address the limitations experienced in current government-sponsored cybercrime reporting websites.

9.1 Participants

A total of forty (40) participants participated in the usability test, randomly selected as a sample representation of those who are most likely to use an Internet reporting

service for cybercrime offences. In addition, the participants were mainly from university students aged 23 – 26 and some adults from different job areas aged 25–35, so that there was variation of not only occupation but also their demographic backgroundThis decision was intentional in order to enable the evaluation process to capture the user's perception with respect to younger, tech-savvy individuals and older, more experienced ones, representing a wide range of citizens who may be required to report cybercrimes in Bangladesh (Table 9.1) (Figure 9.1, 9.2, 9.3).

Table 9.1: Demographic of Participants (40)

Serial No.	**Gender**	**Age**	**University/ Place of Work**	**Occupation/ Field of Study**	**Knowledge About CyberCrime**	**Willingness to use a Government reporting service (If it actually works)**
1	Female	24	Dhaka University	Student (Social Science)	In-Depth Knowledge. Faced Financial Fraud (Credit card Scam)	I will use it if it has good reviews, but I will not use it for finance-related issues.
2	Female	23	BRAC University	Student (Computer Science & Engineering)	In-Depth Knowledge. Faced online harassment. Instagram ID was hacked	I would definitely use it if it can actually solve my issue and catch the culprit.
3	Female	24	BRAC University	Student (Computer Science & Engineering)	In-depth knowledge	I will use it if the website is not slow or crash-prone and if it ensures data safety (no leaks).
4	Female	27	North South University	Research Assistant (ML Field)	In-depth knowledge	I will use it but need several factors checked like data safety, authentication, and tracking.
5	Female	31	Shaheed Suhrawardy Medical College & Hospital	Doctor	Familiar	Depends on the situation; I am skeptical about how well law enforcement can handle online reports.
6	Female	33	The Premier Bank	Banker	Familiar	Except for financial issues, I would use it for other cybercrime-related problems.
7	Female	24	Dhaka University	Student (Social Science)	Familiar	Depends; I might use it for online fraud or harassment.
8	Female	24	North South University	Student (Bachelor's of Business Administration)	Familiar	Yes, I will use it — visiting a police station is a hassle for me.
9	Female	24	North South University	Student (Bachelor's of Business Administration)	In-depth Knowledge	I will use it if it keeps my data safe and actually takes action on my complaint.
10	Female	24	BRAC University	Student (Computer Science & Engineering)	In-depth knowledge	If it ensures data safety and is easy to access and hassle-free, I will use it.
11	Female	25	BRAC University	Student (Computer Science & Engineering)	In-depth knowledge	I will use it if the site is stable, ensures data safety, and is easy to access.
12	Female	26	Daffodil International University	Lecturer (Marketing)	Familiar	No. I do not think I will use it; in our country, in-person cases are rarely solved, let alone online ones.
13	Female	28	Shaheed Suhrawardy Medical College & Hospital	Doctor	Familiar	Lower chance I will use it; shifting fully online will take more time here.
14	Female	28	BRAC Institute of ED	Staff Researcher	Familiar	Depends on the situation; probably not.

Serial No.	Gender	Age	University/ Place of Work	Occupation/ Field of Study	Knowledge About CyberCrime	Willingness to use a Government reporting service (If it actually works)
15	Male	29	Optimizely	Software Engineer	In-depth knowledge	If the complaint process is not lengthy and it ensures safety and actually works on issues, I will use it.
16	Male	23	Daffodil International University	Student (BBA, Management)	Familiar	If law enforcement handles issues better through it, I will definitely use it.
17	Male	23	Daffodil International University	Student (Computer Science & Engineering)	Familiar	No, I won't; I do not trust online processes much.
18	Male	25	MAIS Industries Ltd.	Marketing Consultant	In-depth knowledge. Faced sextortion scam online	Yes, I will use it, but only if the website gains my trust first.
19	Male	26	Optimizely	Junior Machine Learning Engineer	In-depth knowledge	I might not use it; I am skeptical that the police can help via online reporting.
20	Male	23	BRAC University	Student (Computer Science & Engineering)	In-depth knowledge	Yes, if it is hassle-free I will use it.
21	Male	23	Skysonic Aviation	Pilot Trainee	Familiar	Yes, I will use it if my data is protected and not leaked.
22	Male	25	Independent University, Bangladesh	Student (Bachelor's of Business Administration)	Familiar	High chances I will not use it; I think our country lacks capable systems.
23	Male	28	Nagad	Software Engineer	In-depth Knowledge	Yes, I will use it; the police station is a hassle for me.
24	Male	23	BRAC University	Student (Bachelor's of Business Administration)	Familiar	Yes, I might use it for harassment or social media crimes, but for serious issues I prefer in-person complaints.
25	Male	23	North South University	Student (Bachelor's of Law)	In-depth knowledge. Also knows about the cybercrime Laws of Bangladesh.	I might use it, but I think many citizens have low digital literacy so adoption may be low.
26	Male	25	BRAC University	Student (Bachelor's of Law)	In-depth knowledge. Also knows about the cybercrime Laws of Bangladesh.	Depends on the issue and the solutions the website provides.
27	Male	25	University of Asia Pacific	Student (Computer Science & Engineering)	In-depth Knowledge. Faced issues like Facebook accounts got hacked	No, I will not go online for these issues; this is an administrative problem that needs fixing.
28	Male	33	Shaheed Suhrawardy Medical College & Hospital	Doctor	Familiar	Yes, if a dedicated website actually helps, I would use it but only for social media related issues. For major crimes I will not go online.
29	Male	25	AIUB	Student (Computer Science & Engineering)	Familiar	Depends on the severity of the issue.
30	Male	26	BRAC IT	Software Engineer	In-depth Knowledge	I might use it; I have low trust in the system but would if it meets criteria like data safety and official effort.
31	Male	26	AUST	Student (Internet Protocol)	In-depth Knowledge	Yes, I will use it.
32	Male	27	Self Employed	Business Individual	Familiar	Yes, I will use it if it has a good review from a trustworthy source.

Serial No.	Gender	Age	University/ Place of Work	Occupation/ Field of Study	Knowledge About CyberCrime	Willingness to use a Government reporting service (If it actually works)
33	Male	28	Marine Hive Ltd.	Marine Engineer	In-depth Knowledge	I might use it; depends on the situation and its depth.
34	Male	25	BRAC University	Student (Computer Science & Engineering)	Familiar	Yes, if it helps me I will.
35	Male	23	Bangladesh Army	Cadet	Familiar	No. I won't — I do not trust the system and worry about data safety issues.
36	Male	26	Impressive Group	Senior Marchendiser	Familiar	Yes, I will for minor issues; for major ones I will not.
37	Male	27	BJIT	Intern Software Engineer	In-depth Knowledge	If the website is well-versed, I will use it.
38	Male	32	Advance Attire Ltd.	IT Technician	In-depth knowledge. Faced this and went through the legal procedure.	If Bangladesh law enforcement actually works on complaints filed online I might use it.
39	Male	36	Advance Attire Ltd.	IT Technician	In-depth knowledge.	Yes, I will.
40	Male	30	Advance Attire Ltd.	IT Technician	In-depth knowledge. Faced this and went through the legal procedure.	Yes, I will use it.

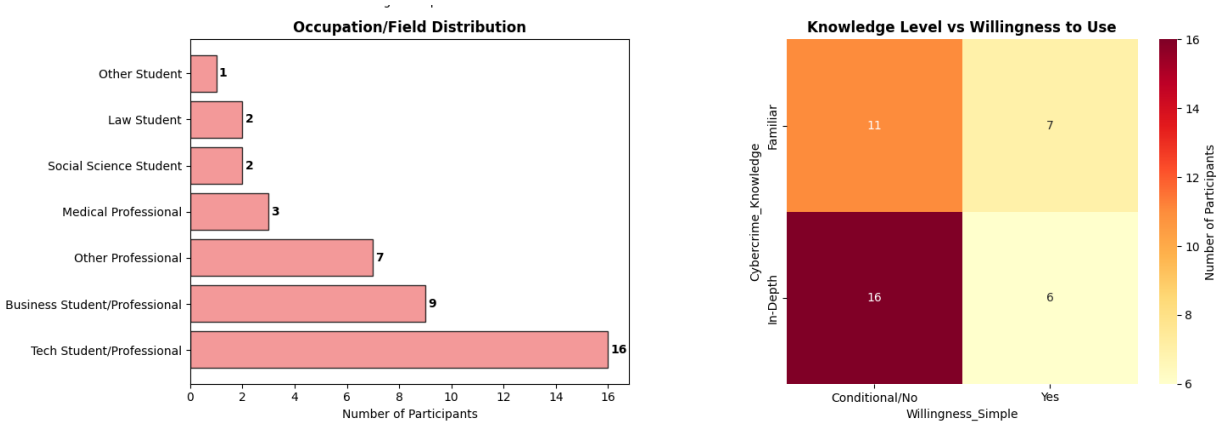

Figure 9.1: Participants Demography

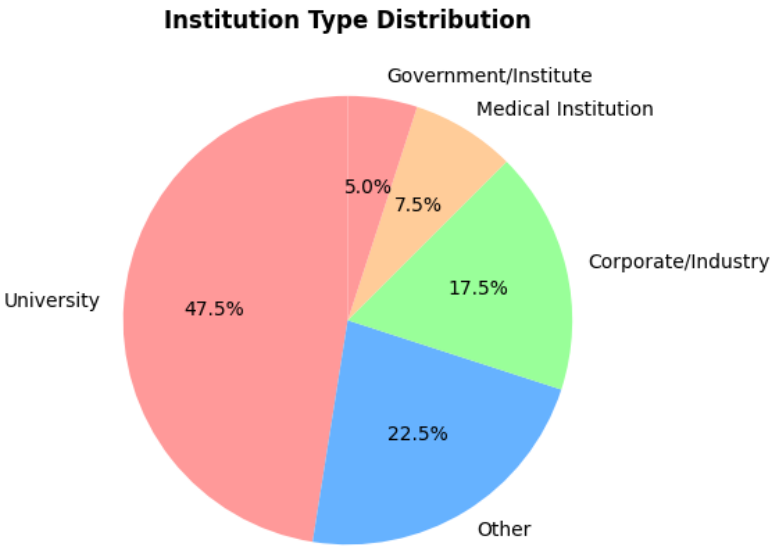

Figure 9.2: Participants Demography

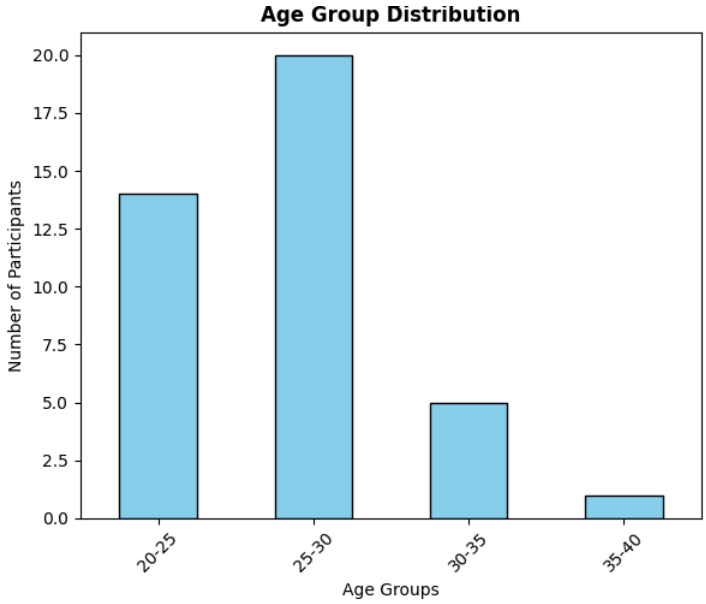

Figure 9.3: Participants Demography

9.2 Testing Setup & Method

The tests were conducted using a moderated user test method, with a researcher present in the session to guide participants, observe their interactions, and understand how they express their thoughts. This approach was taken because it offered a deeper understanding of user experience than unmoderated testing would have done,

because the moderator could prompt participants for any issues they were experiencing while carrying out a task, ask follow-up questions if required and understand not only what the participant said but also interpret their non-verbal behavior (e.g., pauses or body language). As a result, detailed user expectations and obstacles as well as desired value of the system was obtained for the researchers.

Evaluation was performed under controlled conditions for comfort and repeatability. Student sessions were administered in computer labs with internet access on the university campus. Professional tests were completed either in their offices or in a quiet room secured for testing with reliable Internet Access. Participants were invited to complete a subset of dummy and realistic scenarios, such as reporting an online scam or threat, on the proposed website. As the system was a proof of concept and not yet in operation with any government agency, all data were fake, and users were presented with dummy reports and acknowledgement messages. Experimenters used personal computers and cell phones to carry out tasks, along with browsers such as Google Docs to take notes.

9.3 Tasks Performed by Users

For usability evaluation, moderated testing was used to evaluate our website. As we deployed our website on Vercel, it became very easy for us to manage multiple interfaces. As moderators, we were on the admin site to handle issues and have assigned various tasks to our users. Our website features three distinct departments to address users' concerns, including the Financial Department, the Cybercrime Department, and the Fraud Department. We gave each user different tasks. The first task required users to initially create their personal account, which included their NID number or birth certificate number, as well as selfies, and then attempt to log in to the website. Users can only log in after admin approval, so as a moderator, we played the admin role. After approval, users log in with their email address and password, which they used during account creation. Then they were given three to four scenarios (e.g., someone hacked your Facebook account or harassed you online, and now you want to complain about this issue using this website). Another one was (e.g., you faced financial fraud, or someone threatened you to take your money through a credit card or Bkash). So they pick those dummy scenarios and filed a complaint on the website. They had to fill out all the boxes in the complaint file so it could be observed how each user handles the complaint form. Additionally, some provided instant feedback, while others offered input later. Users also found the investigation tracking system interesting and can easily track their complaint updates. Some users faced issues, so for communication, they use a real-time chatbot, where they communicate with both the admin and the AI bot. Then, users explored the additional features, including the Fraud type, About section, and News section. Some users explore those sections before placing a complaint, while others do so after. Those scenario-based tasks helped each user navigate the proposed website. Every user tried to explore every functionality within their capability range. Many users were able to navigate the website easily and use it effectively, while a minimal number of users encountered difficulties navigating the site completely.

9.4 Findings

The proposed website's usability evaluation findings shed light on many features that overcome the shortcomings of existing websites, such as CID, DSA, BTRC, and online GD. Forty users (14 female and 26 male) participated in a usability evaluation of the proposed cybercrime reporting website, providing valuable insights into their user experience with the system.Overall, the users stated the website was quite good and easy to use, which we were trying to achieve through this solution. They provided much more intuitive and functional findings. Based on both the quantitative usability scales and the qualitative data, users conveyed that the system has great potential. Participants also highlighted some areas to improve in future to make this website more user-friendly.

Website Navigation and Feature Findability:
One of the main concerns of the site was to have overall ease of navigation and findability. The majority of the respondents said that the site was user-friendly and simple to use. One participant noted:

> "This site is very straightforward which I liked. After creating an account, it goes right to the complaint file, anyone should be able to navigate it." – Male, 29, Software Engineer

Among 40 users, 34 managed to find the "Report Now" feature. Some confusion was however felt by six users as to where to access the reporting form. Also, three participants were using the search buttons within the "Fraud Type", "News", "About Us" and found these to be overwhelming. On the other hand, 17 participants praised "Fraud Type" feature:

> "I like the presence of an educational section that will make people learn of such crimes,its quite interesting" – Male, 26, Software Engineer

Although the majority of the users appreciated the system, there were people who felt that the non-tech-users or less digital literate people might face some issues navigating this website.

Registration Approval & Investigation Tracking System:
For thirty-one users the registration process was easy and straightforward. Users need admin approval to create an account that creates a positive and safe feeling among users.

> "This feature will exclude fraud users which is good for original users' safety." – Female, 25, Student

But this approval process constrained five respondents in times of emergencies. They showed concern that if someone is in an emergency situation this might become a negative feature for them.

> "It will be extremely frustrating to have to wait before the approval is given in case an urgent case comes." – Male, 23, Student

The balancing of safety and usability was proposed (some users indicated the addition of a button on the dashboard that would be labeled with Emergency displayed on the computer screen). Based on the overall response, post registration approval was considered to be a good sign of safety and trustworthiness and at times can be a negative feature.The most popular feature was Report Tracking, which thirty-five respondents considered to be innovative and comforting.

> "The most fascinating one to me was that I could see my complaint without any hassle and no need to call anybody in case I do not want to." – Female, 33, Banker

> "This feature, I have never encountered on a government site and this provides me with assurance that my report will not be lost in the system." – Female, 24, Student

Reporting Form and Chatbot:
The complaint form received mostly commendation due to its simplicity and usability. Thirty-seven out of forty respondents answered it to the fullest extent, but there was certain confusion over the section of the Department:

> "Overall nice website. However, the dropdown of selected departments was difficult to choose." – Male, 26, Marine Engineer

The chatbot was well-received, as eighteen participants liked that it is available. Nevertheless, it was advised to improve them, such as the emergency prompts and emergency helpline numbers.

> "The chatbot should have a clickable button that reads a helpline to ensure that in cases of emergencies, I do not have to search for the button on the contact section." – Female, 27, Research Assistant

Eight respondents remarked that the chatbot responses at times were less conversational as they were too simplified and limited.
Combined, these findings lead to the acceptability and utility of the tested site across dissimilar groups of respondents. Nevertheless, there were some recommendations to make these sites more useful for a broader target audience. Although users found it to be easy, intuitive and effective. However, some of the features like confusing news sections and feedback issues are evidence that there need to be further iterations. For this developers have to work continuously on the website. Overall, the verdict from the testing was this website has potential that extends beyond being just an online system, it could even be a national solution for cybercrime reporting system.

9.5 Usability Evaluation Metrics (Proposed Website)

For data collection each of the participants was exposed to a given number of dummy tasks, which mimicked real-life development and testing scenarios. These entailed opening an account and completing a dummy report by way of this site. These

exercises were done to gain in-depth feedback regarding the functionality of the site and clarity, efficiency, and satisfaction regarding several features. Standard evaluation measures are used to gain quantitative usability scores as well as to obtain qualitative impressions. Among the several available tools to measure usability, two have been selected to conduct this study because they are particularly reliable and can be used to complement each other: the System Usability Scale (SUS) and the Affinity for Technology Interaction (ATI) scale. A short but adequate assessment of the perceived usability of the proposed websites was given by the SUS. Conversely, the ATI scale disclosed details concerning the predisposition and the comfort of using technology of the users, in general. This twofold strategy would fit well in the situation of Bangladesh, where users can be both digital and non-technological.

9.5.1 Simplified Usability Questionnaire (SUS)

The Simplified Usability Questionnaire (SUS) is a widely used general usability scale for measuring usability purposes [57]. This scale uses points ranging from 1 to 5. Where one(1) represents strongly disagree and five (5) strongly agree.
It comprises ten questions presented in an alternating positive negative rotation, designed to minimize the likelihood of participants responding as they think others would like them to. Their scores are converted into a 0–100 scale using a standard scoring method, with the higher score representing better usability. [58],[57].
The SUS score was used in our study as a simple, reliable, and valid technique that can be applied even with small sample sizes. Studies show that the scale has high internal reliability (Cronbach's alpha 0.9), and is sensitive to differences in usability among product classes ranging from consumer software, business applications, and public websites[57]. Furthermore, previous research has shown that experience can also affect SUS scores, as users with more knowledge or experience in a domain generally report higher usability scores. The Effect of Experience on SUS is even more pronounced in the present study, as participants had varying base levels of digital literacy.[58]
System Usability Scale responses were collected from 40 users after they had thoroughly gone through and used the proposed website. After collecting the responses, they were converted into standardized SUS scores by following Brooke's scoring procedure [57]. To find SUS scores, we need to subtract the odd-numbered questions, such as (1, 3, 5, 7, and 9), by 1. Furthermore, the even-numbered questions (2, 4, 6, 8, 10) are minus from 5. After obtaining these scores, they were summarized and divided by 2.5. After completing this procedure, each participant's scores ranged from 0 to 100 (Table 9.2) (Figure 9.4, 9.5).
So, let us assume,

$$A = (\text{Response Score From User} - 1)$$

$$B = (5 - \text{Response Score From User})$$

Final Formula used here is:

$$\text{SUS Score} = (A_1 + A_3 + A_5 + A_7 + A_9 + B_2 + B_4 + B_6 + B_8 + B_{10}) \times 2.5$$

By using this formula, the SUS Score for each user is given below;

Table 9.2: SUS Score for Each User

No.	Gender	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUM	SUS
1	Female	3	4	4	2	4	4	4	4	4	3	36	90
2	Female	2	3	2	4	2	2	3	3	3	3	27	67.5
3	Female	3	3	3	4	4	4	3	4	4	4	36	90
4	Female	4	3	3	3	4	4	4	4	4	4	37	92.5
5	Female	2	4	4	3	3	3	3	4	3	2	31	77.5
6	Female	0	4	4	4	4	4	2	4	3	2	31	77.5
7	Female	1	4	4	4	3	4	2	4	2	3	35	87.5
8	Female	0	4	3	3	3	3	2	4	3	3	28	70
9	Female	2	4	4	4	3	4	3	4	3	4	35	87.5
10	Female	1	3	2	2	3	3	2	3	2	3	24	60
11	Female	4	4	4	4	4	4	3	4	4	4	39	97.5
12	Female	2	4	3	4	3	4	1	4	3	4	32	80
13	Female	0	4	4	4	3	4	4	4	4	4	35	87.5
14	Female	2	4	3	3	3	3	2	4	2	4	30	75
15	Male	4	4	4	4	2	3	3	2	4	2	32	80
16	Male	2	3	4	4	2	1	3	3	4	4	30	75
17	Male	4	4	4	4	2	4	4	4	4	4	38	95
18	Male	4	4	4	4	4	4	4	2	4	4	38	95
19	Male	4	4	3	4	4	0	4	4	4	3	34	85
20	Male	4	4	4	0	0	0	4	0	4	0	20	50
21	Male	4	4	4	4	4	4	4	0	4	4	36	90
22	Male	0	2	2	3	3	2	2	2	1	3	20	50
23	Male	4	4	4	4	4	4	4	0	4	3	35	87.5
24	Male	3	3	3	4	2	3	4	4	3	4	33	82.5
25	Male	4	0	4	0	4	0	4	0	4	0	20	50
26	Male	4	4	4	4	4	4	4	4	3	4	39	97.5
27	Male	4	4	4	4	3	3	4	3	4	3	36	90
28	Male	4	0	4	0	4	0	4	0	4	0	20	50
29	Male	3	4	3	2	2	4	3	3	3	3	30	75
30	Male	4	3	4	4	3	3	3	4	4	3	35	87.5
31	Male	4	4	3	4	4	3	4	2	2	4	34	85
32	Male	2	3	2	4	3	3	2	4	2	4	29	72.5
33	Male	0	4	4	4	2	4	2	4	4	4	32	80
34	Male	2	3	2	4	2	3	3	4	2	3	28	70
35	Male	1	4	4	4	3	4	4	4	4	4	36	90
36	Male	1	1	4	3	3	4	3	4	3	4	30	75
37	Male	1	4	4	4	3	3	1	3	4	4	31	77.5
38	Male	2	4	4	4	3	3	2	4	4	4	34	85
39	Male	1	4	4	2	3	3	1	4	3	4	29	72.5
40	Male	1	4	4	4	4	4	3	4	4	4	36	90

Now the average SUS score of all the 40 participants are;
Total Sum of SUS Score of each participants are ($\sum x_i$): 3177.5
Total Participants (n): 40
Average SUS Score ($\bar{x}$) = Total Sum of S ($\sum x_i$) / Total Participants (n)

$$\bar{x} = \frac{3177.5}{40} = 79.4375$$

According to SUS, a score above 68 on the SUS indicates above-average usability, and a score exceeding 80 represents excellent usability [57]. The SUS score for the proposed website is 79.44, which exceeds the proposed cut-off point (68). It can be concluded that the proposed website's usability is above average, indicating that users found it fairly easy to use.
Now, the highest SUS score was 97.5 and the lowest score was 50. The mean found was 79.44 (approx). So,
Sum of squared deviations (SS) is:

$$SS = \sum_{i=1}^{n} (x_i - \bar{x})^2 = 6756.09375$$

Population variance & standard deviation:

$$\sigma^2 = \frac{SS}{n} = \frac{6756.09375}{40} = 168.90234375$$

$$\sigma = \sqrt{\sigma^2} = \sqrt{168.90234375} \approx 12.996243447627473$$

Sample variance & standard deviation :

$$s^2 = \frac{SS}{n-1} = \frac{6756.09375}{39} = 173.23317307692307$$

$$s = \sqrt{s^2} = \sqrt{173.23317307692307} \approx 13.161807363615495$$

To identify how spread out the SUS scores are, we need to find the Standard deviation of the scores. SD found for this data set is 13.55(approx), which falls between 10 and 15. Standard SUS research shows that standard deviations between 10 and 15 are moderate variation.[57] As the SD value is 13.55, this implies that not all users experienced similar kinds of issues. For some, the website was more usable; on the other hand, some user groups faced usability issues. According to the SUS standard, High usability is SUS 80.3, Average usability is 68 SUS $<$ 80.3, and Low usability is SUS $<$ 68. Among these data sets, 16 participants had SUS scores above 80.3, 12 participants had SUS scores between 68 and 80.3, and 12 participants had SUS scores below 68.

In conclusion, we found that the SUS (n = 40) had a mean score of 79.44 (SD = 13.55). As per the standard, this is indeed higher than the average usability level that's worth an excellent. However, when classifying students' ratings of usability, 16 users (40%) assigned the system a high usability score, 12 students (30%) an average score, and another 12 users (30%) a low usability score. This spread of inconveniences means that, although the system is usable by the overall majority of users, there are still a significant number of people who have been challenged. The high standard deviation reflects the variation in this, indicating that usability is not uniform for all types of users.

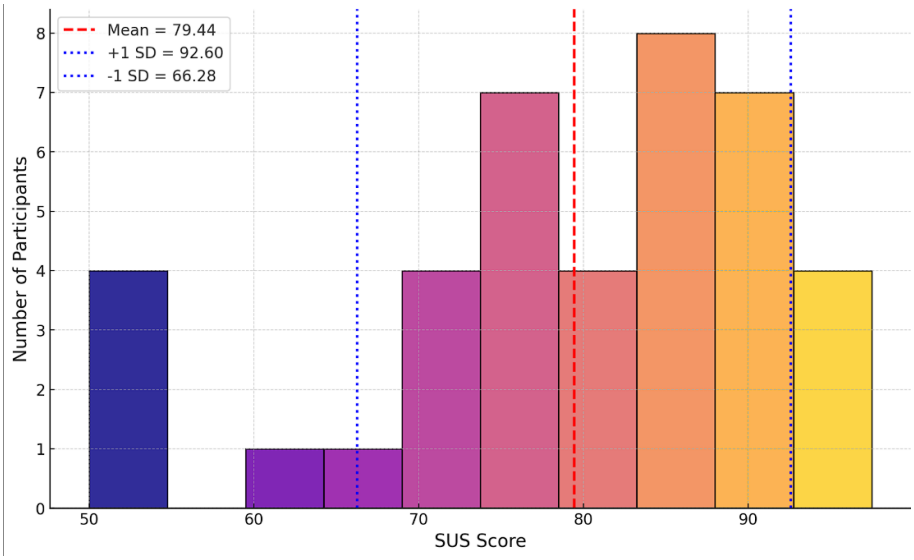

Figure 9.4: Distribution of SUS score

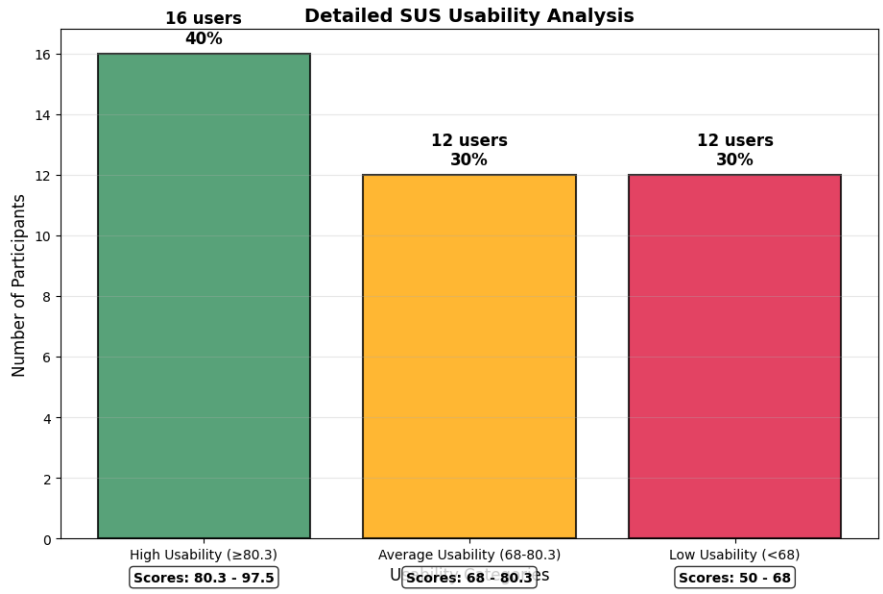

Figure 9.5: SUS score chart

9.5.2 Affective Technology Interaction (ATI)

The SUS reflects perceived usability, but it does not provide insights into individual differences in users' overall adoption of technology. For this reason, the Affective Technology Interaction(ATI) scale was introduced in this study. To measure how different users perceive technological systems and whether they are willing to use them. Affective Technology Interaction (ATI) is conceived as a psychometric scale measuring the general disposition of users to interact with technology actively.[59] Unlike usability oriented measures, the ATI measure indicates users' characteristics or desire to use technological systems. The ATI scale includes nine items rated from

one to six. Here, one represents complete disagreement, and six represents complete agreement. This scale also uses reverse-coded questionnaires(3,6,8).
Higher ATI scores indicate a stronger affinity and openness, whereas lower scores represent apprehension toward digital tools. This difference is particularly relevant in the case of Bangladesh. Because digital divides persist between age groups and occupations here. Even in the 21st century, many people here do not own personal smart electronic devices and view the internet as a place where people can be harmed or where there is a norm of internet use. By combining ATI with SUS, the user's baseline degree of technology affinity can be used as a covariate to control for differing technological attitudes when interpreting usability perceptions. The ATI scale has good psychometric properties (Cronbach's alpha = 0.85) and is predictive of technology adoption behavior.[59] Incorporating it into user testing enables us to determine whether negative evaluations people make of a system are based on actual interface design mistakes or whether they are unwilling to use digital systems in general.To find ATI scores, we need to subtract the "Reverse Coded" questions, such as (3, 6 and 8) from 7. The rest of the question's response will stay as it is. After obtaining these scores, they were summarized and averaged. After completing this procedure, each participant's scores ranged from 0 to 6(Table 9.3) (Figure 9.6). So, let us assume,

$$A = \text{Response Score From User (1,2,4,5,7,9)}$$

$$B = (7 - \text{Response Score From "Reverse Coded Questions"})$$

Final Formula used here is;

$$\text{ATI Mean Score} = \frac{A_1 + A_2 + B_3 + A_4 + A_5 + B_6 + A_7 + B_8 + A_9}{9}$$

By using this formula, the ATI Score for each user is given below;

Table 9.3: ATI Score of 40 Participants

No.	Gender	Q1	Q2	Q3 (R)	Q4	Q5	Q6	Q7 (R)	Q8	Q9	Sum	AVG
1	Female	6	5	1	4	4	2	3	2	5	32	3.56
2	Female	4	4	4	4	4	4	4	3	4	35	3.89
3	Female	6	6	1	6	6	5	6	3	6	45	5
4	Female	3	2	6	2	3	3	4	3	5	31	3.44
5	Female	4	1	4	2	3	2	3	5	2	26	2.89
6	Female	1	2	2	6	6	1	4	3	3	28	3.11
7	Female	4	2	4	1	3	4	4	3	2	27	3
8	Female	1	3	3	1	3	3	1	3	2	20	2.22
9	Female	3	3	2	1	2	1	1	1	2	16	1.78
10	Female	6	1	3	4	3	1	3	2	5	28	3.11
11	Female	4	1	2	3	3	4	3	5	1	26	2.89
12	Female	4	2	4	2	4	4	3	4	3	30	3.33
13	Female	2	2	2	2	2	2	2	2	3	19	2.11
14	Female	4	2	2	3	3	4	3	3	3	27	3
15	Male	6	6	4	4	4	1	5	6	6	42	4.67
16	Male	3	6	2	5	5	1	3	4	6	35	3.89
17	Male	3	4	4	3	6	4	5	5	5	39	4.33
18	Male	3	3	4	4	4	6	6	6	6	42	4.67
19	Male	1	6	1	5	5	2	6	2	5	33	3.67
20	Male	6	6	1	6	6	1	6	1	6	39	4.33
21	Male	6	6	6	6	6	1	6	1	6	44	4.89
22	Male	2	3	1	5	2	2	5	3	4	27	3
23	Male	5	5	5	5	6	2	5	2	3	38	4.22
24	Male	3	3	4	3	4	5	4	5	5	36	4
25	Male	6	6	1	6	6	1	6	1	6	39	4.33
26	Male	6	6	5	5	6	3	5	3	6	45	5
27	Male	2	6	3	5	6	3	5	3	6	39	4.33
28	Male	6	6	1	6	6	1	6	1	6	39	4.33
29	Male	6	5	1	6	6	5	5	4	6	44	4.89
30	Male	5	5	3	5	5	3	3	3	5	37	4.11
31	Male	3	6	1	6	5	1	6	1	1	30	3.33
32	Male	4	2	6	2	4	1	2	2	1	24	2.67
33	Male	6	1	6	6	6	6	6	6	3	46	5.11
34	Male	4	4	3	3	3	3	3	4	4	31	3.44
35	Male	6	6	6	6	6	6	6	6	6	54	6
36	Male	5	4	4	4	4	5	5	5	3	39	4.33
37	Male	5	6	6	4	5	4	5	4	4	43	4.78
38	Male	5	3	3	3	5	5	5	6	3	38	4.22
39	Male	4	5	4	4	5	5	4	5	4	40	4.44
40	Male	5	5	6	4	4	5	4	5	3	41	4.56

Now the average ATI score of all the 40 participants are;
Total Sum of ATI Score of each participants are ($\sum A$): 154.870000
Total Participants (n): 40

$$\text{Average ATI Score } (\bar{x}) = \frac{\text{Total Sum of } (\sum A)}{\text{Total Participants } (n)}$$

$$\bar{x} = \frac{154.870000}{40} = 3.871750$$

Sum of squared deviations (SS):

$$SS = \sum_{i=1}^{n} (x_i - \bar{x})^2 = 6008.59375$$

Population variance & standard deviation:

$$\sigma^2 = \frac{SS}{n} = \frac{6008.59375}{40} = 150.21484375$$

$$\sigma = \sqrt{\sigma^2} = 12.25621653488547$$

Sample variance & standard deviation :

$$s^2 = \frac{SS}{n-1} = \frac{6008.59375}{39} = 154.0665064102564$$

$$s = \sqrt{s^2} = 12.41235297638028$$

According to the ATI psychometric scale, scores typically range from 1 to 2, indicating very low; 2 to 3, low; 3 to 4, moderate; 4 to 5, high; and 5 to 6, very high.[60] We got from the dataset that the ATI score is 3.87. According to the psychometric scale, it falls within the moderate to high range. On average, most participants had shown a positive reaction towards technology and expressed interest in and enjoyment of technology usage. On the other hand, the Standard deviation was 0.923 (approx), which means the dataset shows moderate variability. Many users achieved scores of 5 to 6, indicating a very high interest in the technological system. However, there were also a few participants whose score was below 2, indicating very low interest in technology. However, the variation in these data is moderate, not too high or too low. Most participants fall in the "High"(17) and "Moderate"(13) categories. The overall ATI score distribution is as follows:

- Very Low: 1 participant
- Low: 5 participants
- Moderate: 13 participants
- High: 17 participants
- Very High: 4 participants

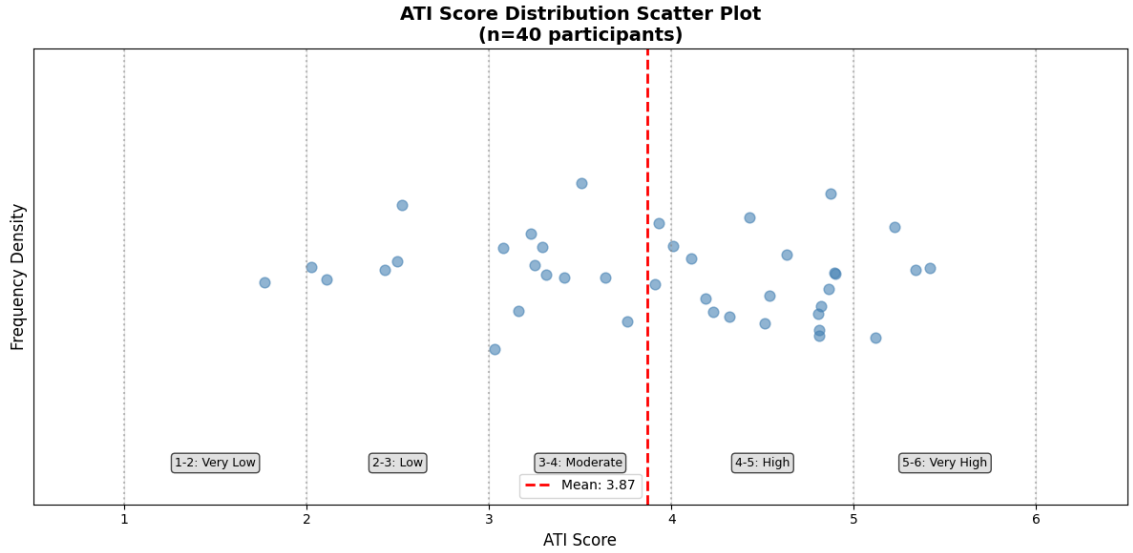

Figure 9.6: Scattered Plot of ATI distribution

And according to gender division the dataset varied as such (Figure 9.7):

Gender / Scale	Very Low (1-2)	Low (2-3)	Moderate (3-4)	High (4-5)	Very High (5-6)
Male	0	1	5	17	3
Female	1	4	8	0	1

Overall the ATIs' results suggested that, in general, participants had positive attitudes toward technological systems, with most falling under the high or moderate categories. Females were skewed towards lower or middle levels of trust, and males mostly fell into the high category (even some very high). It can also happen due to having more male participants compared to females.

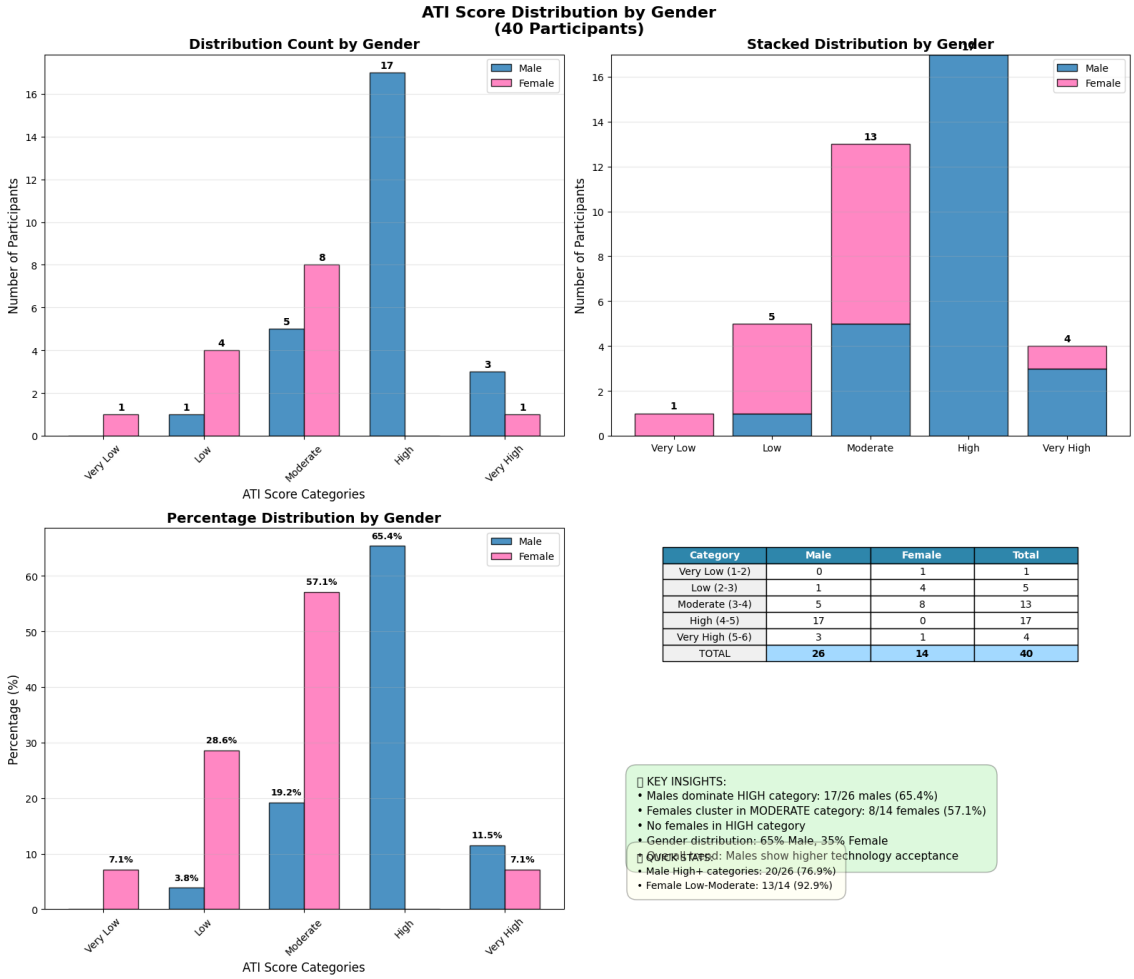

Figure 9.7: ATI Score Distribution by Gender

9.5.3 Synthesized Analysis of SUS & ATI

Two tests (System Usability Scale and Affective Technology Interaction) were used to evaluate the usability of our proposed website, in order to know the perception related to the usability and action preference among users. SUS is a reliable scale for assessing perceived usability, efficiency, and satisfaction. On the other hand, the ATI measures the capability and willingness of users to deal with technical systems.

Analysis of the SUS scores revealed a mean overall score of 71.56, which is above the commonly accepted cut-off point of 68 for good usability. This means that the system was perceived to be, overall, usable and effective; most users reported that they could easily find the complaint form without any hassle. One user stated:

> "It was a very simple website to use, straightforward to the point. I liked it."
> *(29, Male, Software Engineer)*

For almost all users, using the website was easy. They navigated the website very easily, even the non-technical background users. Although most respondents gave positive ratings to the system, a few reported challenges, such as determining the

correct “Department” to select on the complaint form. Two users showed skepticism towards the tracking report system part. These findings show that although the system has not proven to be unusable, there are opportunities for further clarification and simplification.Some of the features proposed by users could also make this proposed site more usable to the users(

The ATI scales, however, provided a mean of 3.56 on a scale of 5 points to indicate that there are quite high stakes of dispositional inclination to communicate with the technology systems. The respondents with greater scores on the ATI scale felt more confident and engaged in searching the system, and this was seen in the increased scores of SUS. Individuals having a lower score in the ATI scale occasionally indicate less usability or lack of confidence, which is a sign of inability and unfamiliarity with technology that is explicable

This observation highlights why user attributes must be taken into account in the evaluation of system performance because the concept of usability is not always understood in a consistent manner at different degrees of technological knowledge.

The pattern can be seen by combining SUS and ATI. The system is usable to most of the users, most especially those with moderate or high levels of technological affinity. In the meantime, they also identify features of the clouds that will create somewhat of a learning curve on the technologically less knowledgeable users. These results of concordance confirm that the system is a high-quality and accessible system in general, but it also allows more and more focused design improvements to make the system more suited to all the groups of users. In general, joint SUS and ATI scores can be regarded as signs of the middle range of applicability, intuitiveness in learning, and acceptance of the suggested version.

A positive relationship between general experience with technology and relative rating of the system determined a positive impact of the latter on such a perspective in participants who reported stronger tendencies of interaction with technology. Most users with even low ATI scores found the system to be easily usable, indicating that it may be suitable for a wide range of users. These findings highlighted the websites' strengths and identified opportunities for further improvement, clarifying areas for next iterations to enhance inclusivity and efficiency in user experience.(Figure 9.8).

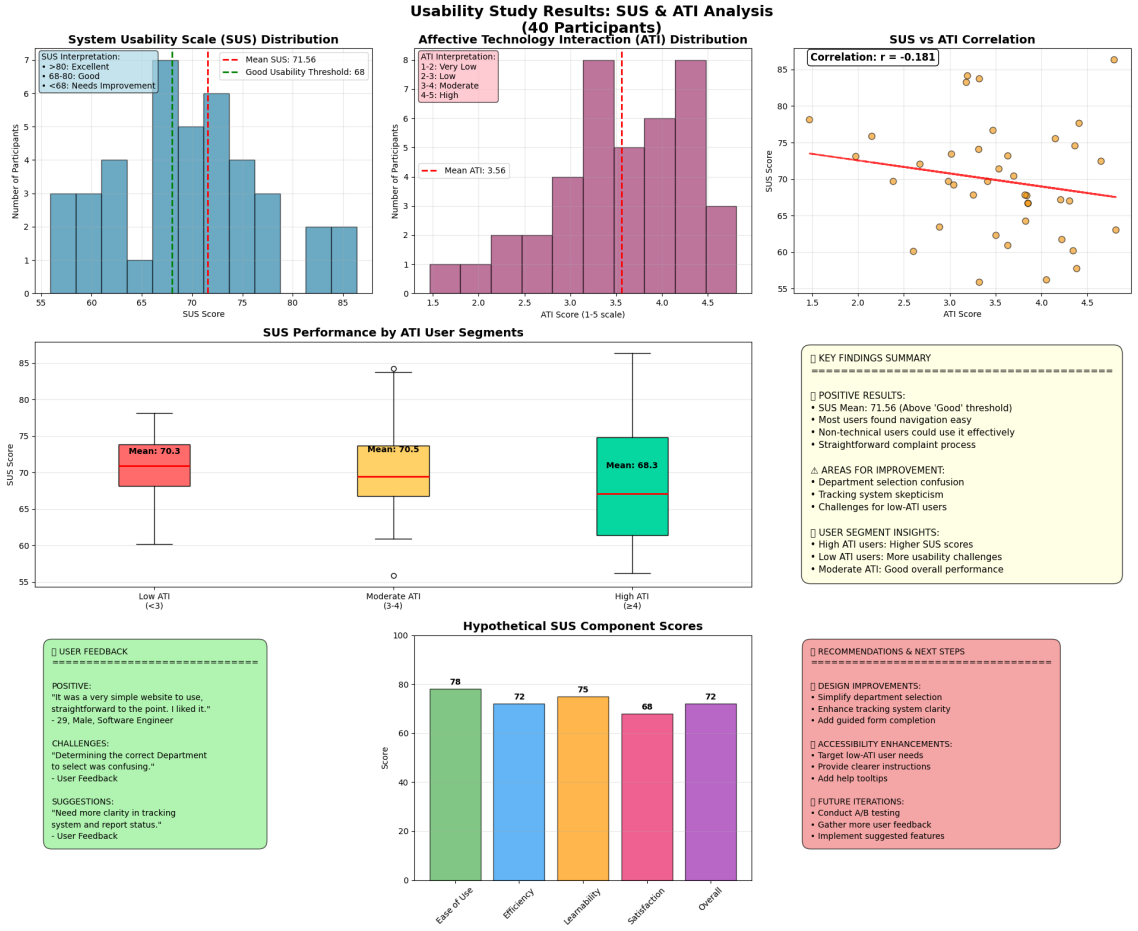

Figure 9.8: SUS and ATI Combine Analysis

9.6 Comparison Between Existing Government Websites Vs Proposed Website

The usability tests of the current government platforms (CID DSA, BTRC, and Online GD mobile app) revealed a poor user experience structure(details in section 4.5) and low confidence in the user's activeness. The later usability evaluation of the new proposed solution website features illustrates both how these challenges could be met and where further design changes are needed. A comparison of the two phases reveals a shift from an outdated system to user-centered systems.

One persistent and frustrating problem with the previous platforms overall was the difficulty in finding and completing complaint forms. No adequate reporting forms were accessible on BTRC & DSA, with the majority of users being referred to external servers in CID.In contrast, almost all participants mentioned that the complaint form was easy to locate and complete in the proposed website "Cybercrime BD". This structured access, with uploaded attachments, details on suspects, and departmental classifications, finally relieved a chronic frustration of vagueness and inaccessibility.

Another important shortcoming is the lack of system feedback. This lack caused

confusion amongst users whether their form has been submitted or not. This not knowing made users skeptical and hindered their usage of these portals. But the new proposed system has a report tracking system. These gave participants reassurance that in which stage their complaint is at.This enhancement significantly improved the usability and reduced confusion associated with task completion.

Another problem that has plagued previous systems was communication; this problem was solved through the integration of a chatbot into the new platform. This system also resolved the previous lack of guidance. Existing government systems were too technical, confusing for users. Conversely, "Types of Fraud" helped users know about what cybercrime is and helped them to gather knowledge about this and use this website more efficiently.

The new programme also resolved the previous lack of orientation and education. Traditional government systems were too technical, confusing users or pushing them away. Conversely, the amount of praise and level of success for "Types of Fraud" as one section and a news center within the intervention suggest a message that promoted better understanding and practical knowledge. Users specifically appreciated these additions for being both knowledgeable and user-friendly. However, some participants suggested that such guidance could be further reinforced by the provision of real-time alerts or a confirming email to get continued assurance after submission.

Notwithstanding these successes, several questions remain unanswered. Some raised concerns with some of the old systems, where data was not encrypted on the email servers. Those fears also linger over the new software system, as the biometric system was not established in the proposed prototype website, and users are hesitant to sign up, fearing that their messages will be stored on a district server forever. Authentication was introduced for credibility purposes, which has gained some praise; however, it raises new concerns by requiring administrative permission before gaining entrance to the system, while also creating a tension between security and expedited safety.They also suggested that a better OTP-based automatic authentication system would make the system more efficient to use.

In summary, the designed system's features alleviate several usability issues that are evident in existing government systems including complaint accessibility,navigation and receiving feedback from the system. Nonetheless, complaints about late approvals, basic chatbot responses, and a lack of follow-up mechanisms suggest that further work is needed on repeat versions of the system. The comparative results suggest that the proposed design provides a suitable foundation for further development of a citizen-oriented cybercrime reporting system. However, it still requires improvement in terms of immediacy, security, and user trust continuity before implementation is anticipated.

Chapter 10

Discussion

This study demonstrated a comprehensive understanding of how Bangladeshi citizens perceive the usability of online reporting systems from an HCI perspective. To gather insight into this, a systematic heuristic and usability testing study was conducted. Additionally, to gain an understanding of how officials address these issues from the administrative side on online platforms, a semi-structured interview was conducted. Overall, these three methodical studies provided us with explanations and clarity about the research question of this study. The significant findings from this study were that usability is a massive issue for the majority of technology users in Bangladesh. If the design, usability, and data security are provided, the majority of literate people in Bangladesh would likely prefer to switch to digital reporting platforms instead of visiting police stations in person. However, people remain skeptical about this and are reluctant to use digital platforms for significant issues, such as financial fraud, due to a lack of trust in online servers for handling confidential information. They also lack confidence in the government's ability to provide such high-tech solutions. On the other hand, the officials who handle these platforms in the backend stated that Bangladeshi citizens have a low literacy rate overall; they still prefer to come to physical stations to solve their issues, so it is not fruitful enough to use that much time, energy, and budget on these platforms to fix it. From the Bangladesh perspective, the usability of online platforms is not the only issue behind the lower acceptance rate of digital systems; the cause of it is rooted much deeper. Issues from the admin side, lack of trust in government, reluctance from the law enforcement side to take action, lower digital literacy among citizens, mental and emotional model, postcolonial computing, sustainability in HCI, cultural and social context, etc., are very important factors to take into account to establish the usability of the digital system following HCI principles in this region.

10.1 Discussion and Key findings

In this section, we present the findings from systematic studies of heuristic evaluations, usability tests, and interviews, as well as the insights this study provides about online reporting systems in Bangladesh as a whole. Each section is relevant to a particular question and provides an overarching interpretation of how the findings address the initial objectives of the study, as well as what this indicates for usability, design, and system administration. It also synthesizes the broader findings of

the research, explaining how each of the stages (user evaluation, system redesign, and offcial's interviews)helped to provide an answer to every one of the five research questions incorporated in this study. It also points out some of the unforeseen results of the analysis process.

10.1.1 Key Usability Issues in Existing Reporting Platforms

First research question of this study was: What are the key usability challenges that users of cybercrime victims face on these systems? To gain insight on this two study heuristic and usability testing was conducted. The main usability issues found in these websites were related to findability, visibility, consistency, flexibility, and design. Users had a difficult time navigating the system and locating the complaint, which was the primary purpose of these platforms. The next issue was visibility; users do not receive any confirmation messages or updates regarding their submission, which created confusion among them. For regular users, understanding the technical terms used in the system, such as (BTRC.DSA), was a challenge. Even some users with a technical background faced difficulties navigating through the websites. These platforms offer limited options for undoing actions or navigating freely. Online GD users cannot edit or withdraw submissions. The DSA platform lacks back navigation options. Adding " Edit," and" Cancel" features. Systems also exhibited inconsistent terminology and layouts. Users uniformly found the CID website to be unusable and unintuitive for task-oriented reporting requirements. Almost all of the users (38 people) who visited the CID homepage found themselves disoriented due to a mismatched layout and a distracting information architecture. Key features for a reporting system, such as filing a cybercrime complaint, were not immediately apparent where they were expected to be. Twenty-nine(29) users were initially confused about where to find the complaint form. These websites initially lost credibility due to their uniform designs and cluttered information presented in one place. Some participants in the usability testing had previously experienced cybercrimes and attempted to use these platforms for reporting purposes. However, the websites did not assist them effectively due to their poor usability. Overall, the heuristic and usability testing yielded results about the key usability hindrances in these existing websites, which include navigation, findability, visibility, design issues, data security concerns, acknowledgment or feedback systems, broken links, lengthy complaint forms, or the absence of complaint forms altogether.

10.1.2 System Designing for diverse users

The second research question aimed to inquire whether a user interface design for a cybercrime reporting portal is capable of serving different types of online users, such as students, employees, medical doctors, and individuals, which can be subdivided into technical and non-technical categories. The user testing of the websites for the Criminal Investigation Department (CID), the Bangladesh Telecommunication Regulatory Commission (BTRC), and the Digital Security Agency (DSA), as well as the Online GD mobile application, provided important insights that directly informed this section. The testing revealed usability, accessibility, and communication barriers that different user groups handle differently, illuminating what capabilities a well-designed system needs to include to serve a broader population more effectively.

Results showed that users with varying educational levels, computer science backgrounds, and internet usage frequencies exhibit different behaviors in the same digital space. The importance of incorporating clear instructions, plain language(Bangla and English) is necessary to not exclude users who are not technically proficient.

Systems does not have user manual and user feedback. Such gaps demonstrate the necessity to have in any kind of systems, particularly in reporting that something is. Another insight is that all users have diverse motivations and emotional stimuli when interacting on these platforms. Younger users liked fast, stripped-down interfaces.But professional users preferred official tone and formality. This calls for a balance between modern and credible usability.

Lastly,inclusion in design also means guaranteed privacy and data protection. Several participants were concerned about where data was held and who could see it. A safer process was suggested to secure the use of National ID or verified credentials, ensuring that both accountability and trust are respected. Such a system would make it difficult to file false reports and would reassure users that their data is being handled responsibly.

In short, user testing on public sites has conclusively shown that a "one-size-fits-all" approach cannot accommodate the diverse needs of people using government digital services. Accordingly, a cybercrime reporting site should have a simple and easily navigable design, a bilingual interface, ease of accessibility, and guidance for users, in addition to ensuring the security of data. These findings have directly informed the proposed solution in this work, incorporating these design concerns and principles to create a more accessible and trusted user platform for citizens of all digital literacy levels.

10.1.3 Administrative and Law Enforcement Perspective

The semi-structured interview study addresses the third research question regarding how law enforcement bodies address technical gaps in online reporting websites in Bangladesh. While a series of user studies recorded evidence of citizen-side friction (in terms of navigation, clarity, and confidence), the interviews explore the backend (websites) in a concise way. How reality (on the backend) becomes something that front-ends can work with was found from interview study.

Interviewees described a broken pipeline for intake at all levels. Managers cannot trust the identity of a user submitting reports (no authorisation), and submissions often go through several handovers. In that process matadats are lost more often. According to them, even if the online system is really good and has high usability still there are high chances that the system would also be unable to get through to the target recipient. As there is no means of verifying the reporter, authenticating the evidence or ensuring that cases are sent for consideration by the appropriate unit. These aren't just technical glitches to be fixed with a software update. The officials said, the structural flaws inside the government operational process are highly

responsible for lower acceptance rate of these systems. Furthermore, it was known through interviews that these weaknesses did not appear after the pandemic.These structural and operational flaws are there for decades and higher ups are not even ready to fix these or acknowledge these.

In many cases, there is no interconnection among the departments and no auditable record of action as case data is further handled differently by the different departments. The reported instances of the critical cases of cybercriminals like phishing, or online harassment are often handled through personal networks and rarely through official means. The government sector lacks the existing standardized, trusted, and secure data and evidence sharing methods. Which causes citizens and admins to lose confidence in the digital direction.

These limitations also affect the interface and workflow of both sides of a system(citizens and law officials). The available platforms do not provide very much direction on what to include, attaching or keeping evidence or not. As a consequence of these, users can never check the status or follow-ups about their report. As a consequence, the victims are more likely to visit the police stations on several occasions. The administrative side shows missing case files due to the lack of systematic triage, shortage of available capable officers who work at different departments, and passing case reports between various departments. And their resources also are seldom found on the official sites. The lack of staffing and training of IT complicates the necessity to provide a reliable implementation of the digital intake that was to be consistent and high-quality.

Officials stated, harassments through facebooks usually happen using VPNs and disposable mobile networks, which demand a rapid and highly integrated framework which the existing systems are not capable of delivering. The interviews are unified around three common causes of all that delay and distrust: fragile verification and routing at the entry level, scattered data and lack of effective data collaboration; interfaces that fail to guide citizens or give officers the power to route people at high speed.

As such the administration informed us that it would require a lot of time to adjust the internal system to put in place an online reporting system. It requires the assistance of the police department internally and a special internet reporting unit. Better data security and listening to investigations also should be incorporated. The management ought to employ and groom additional IT staff as a solution to that problem. Direct digital capture that conserves quality of evidence in addition to secured chain-of-custody; central case management which enables auditable handovers automatically. This can be a smooth process in Bangladesh to its citizens by addressing all the needs of the citizens.

To address the third research question of this study, it can be stated that the online application of a law enforcement system must be congruent with the back-office operation of verifiability, triage, and evidence integrity, or interagency cooperation. Through this two-pronged method, which is a mix of UX and the working side, we may succeed in turning digital reporting into a trustworthy tool to the constituents

and functional to the officers.

10.1.4 Applying HCI Design principles for Improved Usability

Research question four aimed to investigate how the redesigned cybercrime reporting portal enhanced user trust and satisfaction compared with existing government websites previously surveyed. Results from the second usability evaluation, involving SUS and ATI questionnaires, revealed a significantly improved overall user experience with the redesigned interface.

The SUS scores indicates user satisfaction, with users describing easier navigation, clearer labeling, and less cognitive load when performing core tasks, such as submitting complaints, finding information, or browsing legal resources. The recreated system included user-centered features, such as stripped-down menus, visible progress bars, and an investigation tracking system, which targeted specific pain points that arose during the initial testing phase. Therefore, users reported greater trust in the system's stability and professionalism. Nevertheless, they also suggested various types of development areas on the website, such as adding bilingual features (both Bangla and English). The investigation process update should be emailed to the users. Adding information about which department to choose in the complaint form instead of keeping it in a different section. Available options for adding more than one attachment in the "evidence" section of the complaint form, etc. These suggestions provide a future direction for this research study. Keeping this recommendation in mind, further literature work can be conducted. Additionally, continuous development of the website is also necessary, as identified in this study.

On the one hand, the result from ATI indicated that the participants who had high technology affinity levels were more satisfied with the redesign. The logical architecture and enhanced system feedback were liked by a technically proficient group of the participants, but the tools tips and chatbot icons were important to the non-technical users. Such design decisions were also useful in eliminating the fear and panic experienced by some of the users who have always had difficulties browsing the complexity of government websites. This proves that, besides security and authentication services developed, trust is promised by the predictability and user controllability services, another element that was premeditated in the redesign.

Also, the transparency and certainty were also a factor to enhance the level of confidence of the users. According to the findings, enhancing system design would be able to stimulate better user trust and utility through compromising in some aspects with security.This observation shows that user trust relies on the technology's reliability and hearted design decisions can mitigate the user's fears.

10.1.5 Understanding Low Digital Adoption Rate

The second phase usability evolution on the proposed website presented that in terms of usability it was a good solution. A crucial observation was made during Phase 2 of user testing. This finding also explained our final research question whether the usability is enough to make Bangladeshi citizens leave the analogical system and adopt the online reporting system. The results suggest that usability is a prerequisite for digital adoption, but alone not sufficient. In human factors and psychology, more underlying socio-cultural effects and motivators such as the perceived reliability of institutional systems, seriousness to reporting, but also post-colonial attitudes towards digital governance are affecting the design space of user behaviour and acceptance.

Separating "working well" and "being willing to use this type of tool in major issues" kept coming up over the second round of usability testing. Common remarks were: "Usability is acceptable and praisable, but I do not trust online services that much, even if the government provides them." One official remarked that "Not everything should be online; a few things are okay to do online, but crime-related issues should be solved in person." Another user shared, "Financial documents should not be shared online because what if a security breacher?" Several participants also wondered whether the people of Bangladesh were ready for such changes. "I do not think Bangladesh is on a level that people will handle crime online because here law enforcement does not solve crimes offline." From the systemic interview study, it has emerged that officials are aware of citizen's digital literacy. People of our country are not very educated, let alone in digital literacy. Even in a physical police station, they are unable to provide the correct documents. How they will handle online sites is still a dream. According to the study, it can be concluded that many citizens remain "digitally challenged," particularly outside major cities. To establish digital systems in Bangladesh, a significant amount of groundwork needs to be done first. The usability of a system alone will not solve this issue.

To support our study, we were also able to source additional findings from literature existing on this theme in Bangladesh. This is documented in a national-level study which has found low and uneven levels of digital literacy among rural Bangladeshi citizens, contributing to weak uptake of e-government services [61]. The knowledge and skills were also inadequate among rural users, discovered by the survey under BRAC Institute of Governance and Development as being a major reason for the refusal to take part in digital platforms [61]. This observation is consistent with what this study revealed since some participants had the capability to use the proposed website but they were not stretching their limits, and they were anxious to use and operate the interface without any assistance.

The second is the limited use as a result of non-technological barriers. It was identified that 5As: Availability, Affordability, Ability, Awareness and Agency has a strong impact on the users depending on whether they will indeed adopt a digital system or not [62]. Such an apprehension still persists in the digital age even on the internet, another study discovered is that even though the digital platform has modernised customers do not have confidence in digital media transaction method[62].This is the general apprehension of the system, which we had also discovered in our study,

which included sentiments such as (e.g. I do not feel safe dispatching financial materials through the Internet). Hence, we cannot certainly say that an online reporting system would be utilized by all the users of financial fraud cases, as affected by the emotional and cultural distaste to it.

Third, emotions play a crucial role in the process. The information system literature indicates that negative moods (e.g., anxiety, fear, or frustration) can influence intention and the use of digital systems, even in individuals with above-average ability [63]. This may help explain why our participants who described the revised system as "easy enough to use" nonetheless expressed hesitation about using it for actual reporting.

Finally, a postcolonial computing perspective also offers a deeper insight. As Irani et al. claim, design models at the global level often rely on a homogenous rationality that ignores how the contexts of history and institutions influence technology use [64]. For citizens in Bangladesh, who have long turned to physical police stations and in-person accountability as a "mental map" for trust and legitimacy, technology alone cannot replace that. Postcolonial computing serves as a reminder that technologies designed through Western usability logics may challenge local expectations around authority, justice, or social mediation [65].

In short, the findings from this research demonstrate that even in the case of designing and implementing an excellent and highly usable digital reporting system, adoption is partial due to a lack of trust, emotional safety, and Socio-Historical Attention. Usability is a necessary but not a sufficient condition, as deep adoption requires building digital confidence, ensuring privacy and safety assurances, and reconciling new systems with entrenched cultural practices. To understand these interlinked emotional, cultural, and postcolonial dimensions is crucial if Bangladesh is to transform truly digitally.

10.2 Contribution to existing Literature and Research Gaps

This study contributes to the existing body of literature in digital system usability and HCI, particularly in developing countries such as Bangladesh. Although a number of studies have investigated e-government user experience (UX) and usability, most of them prioritised technical efficiency or visual aesthetics over gaining an understanding about the holistic UX journey alongside the socio-technical issues relation to digital service adoption. The findings of this study have extended the work of others by integrating heuristic evaluation, usability testing, administrative staff interviews and Heuristic-informed human computer interaction redesign, to offer an in-depth investigation on the part that can be played by usability barriers and digital adoption behaviour for online reporting systems deployed in Bangladesh.

Earlier studies such as Rahman's study on multi-channel government sites revealed that Bangladeshi websites are not user friendly, less accessible and do not follow

structured design processes [66]. But the study was primarily focused on heuristic and semiotic analysis, which did not particularly follow up with end users or managerial influence. On the other hand our work extends this research by conducting a user centred usability testing also with the admin side. Therefore fulfils an important gap of inclusion and accessibility in digital design. The findings demonstrate that, in addition to the simplicity of interface design, the unambiguity of task flow and the familiarity with language also have more impact on user performance which were not fully explored by prior frameworks.

Similarly, Sattar et al. emphasized the importance of bridging the gap between academic and industry practice in the HCI case of Bangladesh as there is a lack of practices on locally appropriate HCI within real projects [67]. This paper makes this recommendation operational by applying HCI designs like user-centred design and iterative testing, to deploy a system in real-world public service setting; which led to specific benefits in terms of usability and perceived trust. Consequently, it fills the academia gap because it demonstrates how HCI design strategies may be applied to produce new and contexturally relevant digital platforms.

A study conducted by Bidgoli [41] and Pimentel [68] analysed user engagement of awareness campaigns on crime using chatbots and did not take into account the usability of the infrastructural systems that allow interactions. Rather, it is that this research has contributed to our understanding of the underlying processes by which usability design influences reporting motivation and accuracy leading to outcomes in citizen engagement. By filling this gap, this research study enhanced it beyond simple awareness tools like chatbots to redesigning an integrated user interface which citizens can actually use to report incidents. By improved system usability and HCI-informed redesign, this research also showed that higher system usability leads to increased user engagement and trust level. Thus the proposed awareness ideas of Bidgoli [41] and Pimentel et al. [68] are operationalized into a working, user-centric reporting structure in this study.

In the wider scope of usable security, Fallatah [69] developed a model to explain how system usability is related to the culture and the compliance with security of companies. Motivated by this principle, our study hereby illustrates how improved usability in crime-reporting portals could also foster user trust and perception of system security, thus further substantiating the connection between usability and compliance across domains. Hence, the results confirm Fallatah's theoretical proposition in a public sector digital reporting context. Also, a study on the usability of Bangladeshi e-government websites by Shadat and Islam [61] found basic accessibility issues but only covered the structural aspect of usability. The present study takes this line of inquiry to the next level by integrating structural analyses with field-trial behavioral insights, thereby achieving a more "humanized" analysis of interaction barriers. This mixed approach serves to confirm previous findings and to enhance the conception of usability for low-literacy, culturally specific contexts.

Finally, although almost all of the related work, such as Fallatah [69] and Sattar et al. [67] stressed the importance of usability in technological or educational prospective, whereas the current study construes usability as a knowledge construction tool

toward social inclusion in digital governance. By revealing what citizens with low digital capability think of reporting web platforms and by engaging reporting users as well as administrators in iterative design, this work adds to empirical knowledge that usability influences digital adoptions, and trust in governance. Thus, this approach addresses the existing void in e-government research by expanding user diversity and socio-cultural adaptation.

In conclusion, the research builds on existing literature by showing that if usability is improved according to participatory and HCI methods then efficiency improves as well as digital confidence and institutional trust develops. The findings therefore address a crucial gap in the literature on usability, accessibility and acceptance of e-government systems in developing countries.

10.3 Contribution to HCI

This research contribution to the HCI field lies in expanding usability studies to include a developing country setting where digital literacy and technology awareness are minimal. The majority of HCI research has focused on developed countries and technology proficient end users. In contrast, this study provides an empirical account from Bangladesh on how usability guidelines can be enforced in the context of a type of city that is still learning to interact with digital systems. By examining the usability of online crime reporting websites and identifying design issues through heuristic evaluation and user testing, this work expands our practical understanding of HCI in low-resource countries.

The mix of user-level and administrator-level perspectives is also a significant methodological contribution. HCI efforts on governance usually focus on the user-centered experience, without frequently paying much attention to the effect of institutional and administrative receptiveness on the performance of the system. Interviewing users and admins, this study will offer two-level opinion on usability with the back-end and front-end effectiveness and utilization being mutually reliant. This perception is very critical in regards to the emergence of the digital government system, which serves both the citizens and the government officials that serve the people. Moreover, this paper helps justify the use of HCI towards development that can be achieved by illustrating the ability of heuristic and usability assessment techniques to identify implementation-friendly design refinements to developing nations, such as Bangladesh. Along the way, it will provide the contribution of HCI in the application of accessibility, which in turn eventually leads to digital inclusion, and partially remaking government online reporting systems into the digital environment, is brought into focus.

All in all, the research would be a great contribution to the literature in HCI as it puts the context of the usability evaluation in a developing country, bridges citizen and institutional experiences, and shows that rigorous implementation of HCI techniques can educate the architecture of smarter and more inclusive e-governmental platforms.

Finally, the results of the study are interpreted based on the study objective and research questions in this section of the paper. The research findings were as follows conducted through heuristic reviews, usability testing and interviews with administrative staff that revealed the application of HCI principles and augmentation of usability can help in boosting adaptability and user satisfaction. Nonetheless, this research established that the developments are not always adequate in giving confidence regarding the full scale application of the system. The online reporting system is dependent on both the institutional preparedness, trust, digital literacy, and integration of the user experience and operational capacity in Bangladesh. Overall, the paper shows that digital transformation in public reporting has more than just the technical usability but should be viewed through the scope of social inclusion.

Chapter 11

Conclusion

This chapter summarize the main results and contributions of the study. And also, the limitations of research, and the future work. We explore the usability challenges based on the real-world of the existing system in Bangladesh. For example, CID, DSA, BTRC, and the Online GD application. We actually use a mixed methodology approach for evaluating the existing websites and applications, which includes user-testing, Heuristic evaluation, and semi-structured interviews. Then we design a user-centered prototype that facilitates task completion, feedback, status clarity, perceived usability, and the communication process. It proves that employing HCI principles is exactly what the end user expects. Then, language, diversity, visibility into system status, error prevention, and helpful guidance are simply designed to build confidence by isolating reporting touchpoints. Also, not only does it translate into a seamless citizen journey, but it also reduces downstream friction for investigators.

11.1 Summary

This study evaluates the essential usability problems found with current cybercrime reporting systems in Bangladesh. We utilized a systematic diagnosis to characterize the failures of Bangladesh's cybercrime reporting channels, namely CID, DSA, BTRC and the Online GD app in succeeding actionable citizen intent, and further translated those insights into an HCI-sound prototype assessed against standardized instruments and qualitative feedback culminating in empirically measurable usability improvements along dimensions of discoverability, guidance as well as transparency of case progress. Mixed methods were at the core of the: 40-person task-based user testing exposing critical failures including disorientation on CID, the absence of any online complaint form on DSA and BTRC, app crashes and OTP issues on Online GD, and a universal lack of tracking/confirmation, five expert heuristic evaluations mapping failures against Nielsen's heuristics (visibility status, recognition rather than recall, error prevention, help and documentation), and semi-structured interviews with key officials contextualizing bottlenecks in verification, inter-agency handoffs, data sharing, and staffing constraints that currently force many victims back into in-person reporting. These included the operationalization of plain language and progressive disclosure, inline validation, tone settings to provide accessible language toggles, and a single location for tracking current status; followed by significantly higher SUS and Affective Technology Interaction

(ATI) measures for perceived usability and affective comfort, including particularly strong user feedback on guidance related to the capture of the evidence, and clarity about what occurs after submission—one of the strongest trust levers in play for low-literacy and mixed-connectivity contexts. The triangulated findings indicate that reconfiguring interaction journeys and feedback loops rather than simply adding technical functionality reduces abandonment and evidentiary quality and aligns public expectations with agency workflows, enabling greater throughput for investigators and restoring confidence in digital-first reporting.

11.2 Limitation

There are three limitations that bound interpretation and generalization. Second, while the participants are diverse in profession and experience, a patterned divergence on ATI: non-tech participants gave much lower ATI scores than their tech counterparts, and non-tech users gave much higher ATI scores than their more confident tech users, suggests both an affective gap (i.e., an unwillingness to adopt based on design experiences) and a confidence gap (i.e., an actual inability to convey the appropriate response based on technological capability) that design will have to address explicitly in a literacy-aware manner with scaffolding, multimodal inputs, and simplified terminology; this also suggests an urgent need for larger samples of non-technical users across regions and languages, to minimize bias and to make a better estimate regarding comfort, adoption, and acceptance of the redesigned flow at the population level. Second, stakeholders' access constrained the depth of 'operational' triangulation; as such, only five in-depth interviews with law or government officials were possible, which impacted our breadth of understanding around cross-agency integrations (e.g., the reliability of NID/OTP verification, shared Case IDs, data-sharing with banks or social platforms), policy bottlenecks, and staffing/training realities that affect back office throughput and response quality. Third, the prototype evaluation, while positive on SUS/ATI and qualitative feedback, was time-bound and scenario-based and did not longitudinally measure sustained trust, real-world abandonment behavior, and resolution timelines-to-load due to peak incident surges, thus requiring field pilots with analytics, follow-ups, and operational SLAs to validate durability and scale.

11.3 Future Work

Future research will focus on the development and testing of the proposed cybercrime reporting platform, with a central emphasis on refining its usability and security features. The platform will be built upon the insights gathered from user testing and heuristic evaluations conducted during this study. The future work will involve an iterative development process. We will introduce diverse participant groups from various demographics. This will help to guide whether the new platform addresses the concerns identified in the current systems. For example, navigation difficulties, form complexity, feedback, communication process, and tracking system. One of the core areas for improvement will be the introduction of multilingual support. It will ensure inclusivity for users with different language backgrounds. Additionally, enhancing the mobile-friendly functionality is essential as people use mobile phones

in everyday life. To improve the overall efficiency, future work will also focus on optimizing the system's performance. This includes exploring scalable solutions to handle higher volumes of traffic and ensuring data persistence. An important aspect of our future work is to propose the implementation of our developed website to the Bangladesh government as a government platform for cybercrime reporting. It will be the government's decision whether to adopt and implement the platform for the betterment of the country's cybercrime reporting system. These future prospects will ensure that the platform develops into a comprehensive, and user-centered cybercrime reporting tool. Our platform will overcome the current limitations.

11.4 Final Remarks

In other words, this thesis demonstrates that usability is not an afterthought, but rather a fundamental element for the effectiveness and credibility of cybercrime reporting in Bangladesh. Where the recovery depends on finding pathways, capturing evidence ,providing predictable identity checks, and visible progress tracking to citizens of varying levels of digital literacy. This work demonstrates that HCI-informed prototypes designed through an inclusive interaction design process. It can reduce dereliction, improve evidentiary quality, and align public expectations with agency processes. It creates some systematic effects: more investigative output, increased confidence level in digital reporting, and diminished post-submission confusion. Institutions adopting inclusive HCI standards, enforcing interoperable status and verification services, embedding continuous measurement across front-stage experience and back-stage operations can make sure the system serves non-technical users as reliably as the technically confident, and thus deliver consistent, timely outcomes when harm occurs.

References

[1] Criminal Investigation Department, Bangladesh, *Cid bangladesh*, https://www.cid.gov.bd/, Accessed: 2025-10-09, 2025.

[2] Bangladesh Telecommunication Regulatory Commission, *Btrc*, https://btrc.gov.bd/, Accessed: 2025-10-09, 2025.

[3] Prime Minister's Office, Bangladesh / Department of Social Services, *Department of social services — pmo portal page*, https://dsa.portal.gov.bd/site/page/bfd1402c-985e-4943-8020-7ac0182533e1/www.pmo.gov.bd, Accessed: 2025-10-09, 2025.

[4] Bangladesh Police, *Online gd — public user access*, https://gd.police.gov.bd/Auth/PublicUser, Accessed: 2025-10-09, 2025.

[5] J. Nielsen, "Enhancing the explanatory power of usability heuristics," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '94)*, Boston, Massachusetts, USA: ACM Press, 1994, pp. 152–158, ISBN: 0-89791-650-6. DOI: 10.1145/191666.191729.

[6] L. F. Cranor, "A framework for reasoning about the human in the loop," in *Usability, Psychology, and Security (UPSEC 2008)*, Full paper at `cranor.pdf`, San Francisco, CA: USENIX Association, Apr. 2008. [Online]. Available: https://www.usenix.org/conference/upsec-08/framework-reasoning-about-human-loop.

[7] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 1990, pp. 249–256.

[8] J. Brooke, "Sus: A "quick and dirty" usability scale," in *Usability Evaluation in Industry*, P. W. Jordan, B. Thomas, B. A. Weerdmeester, and I. L. McClelland, Eds., Originally published June 1996, London: Taylor & Francis, 1996, pp. 189–194.

[9] E. Kirui and P. K. Kemei, "Usability of e-government services in developing countries," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 15, no. 3, pp. 102–107, 2014, Open access, ISSN: 2231-2803. DOI: 10.14445/22312803/IJCTT-V15P123. [Online]. Available: https://ijcttjournal.org/archives/ijctt-v15p123.

[10] M. S. Rana, "A critical analysis of the escalating cybercrime and its impact in bangladesh," *CIFILE Journal of International Law*, vol. 5, no. 9, pp. 40–49, 2024.

[11] R. J. Rony, N. Saliheen, and N. Ahmed, "Cybercrime experiences, handling and practices: A reality check in the perspective of urban bangladesh," *Handling and Practices: A Reality Check in the Perspective of Urban Bangladesh (July 13, 2021)*, 2021.

[12] N. M. Zawad, "Cyber security in bangladesh: An overview of threats and prospects," *Addaiyan Journal of Arts, Humanities and Social Sciences*, vol. 5, no. 01, pp. 1–11, 2022.

[13] M. B. Mollah, S. S. Islam, and M. A. Ullah, "Proposed e-police system for enhancement of e-government services of bangladesh," in *2012 International Conference on Informatics, Electronics & Vision (ICIEV)*, IEEE, 2012, pp. 881–886.

[14] B. G. M. K. Alam et al., "Cybercrime in bangladesh: Implications and response strategy," *NDC E-JOURNAL*, vol. 10, no. 2, pp. 20–35, 2011.

[15] IEEE Security & Privacy, "Virsec: Virtual reality as cost-effective test bed for usability and security evaluations," in *2021 IEEE Symposium on Security and Privacy Workshops (SPW)*, IEEE, 2021. DOI: 10.1109/SPW53761.2021.9419223. [Online]. Available: https://ieeexplore.ieee.org/document/9419223.

[16] G. Tsakalidis and K. Vergidis, "The art of cybercrime community research," *ACM Transactions on Privacy and Security*, 2024. DOI: 10.1145/3639362. [Online]. Available: https://dl.acm.org/doi/10.1145/3639362.

[17] N. Martins and S. G. Correia, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Computers & Security*, vol. 105, p. 102 248, 2021. DOI: 10.1016/j.cose.2021.102248. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404821000821.

[18] K. M. Kuo and B. J. Tang, "Prototyping usable privacy and security systems: Insights from experts," *International Journal of Human–Computer Interaction*, vol. 38, no. 1, pp. 45–62, 2021. DOI: 10.1080/10447318.2021.1949134. [Online]. Available: https://www.tandfonline.com/doi/10.1080/10447318.2021.1949134.

[19] MDPI Sustainability, "Integration of cybersecurity, usability, and human-computer interaction for securing energy management systems," *Sustainability*, vol. 16, no. 18, p. 8144, 2024. DOI: 10.3390/su16188144. [Online]. Available: https://www.mdpi.com/2071-1050/16/18/8144.

[20] O. J. Ndubuisi, G. Adene, B. T. Sunday, C. E. Mbonu, and A. U. Gift-Adene, "Digitally improving uk police surveillance and incidence response using real-time crowd reporting app: Digipolice," *Global Journal of Engineering and Technology Advances*, vol. 18, no. 3, pp. 124–138, 2024.

[21] G. Tsakalidis and K. Vergidis, "A systematic approach toward description and classification of cybercrime incidents," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 4, pp. 710–729, 2017.

[22] S. W. Smith, "Humans in the loop: Human-computer interaction and security," *IEEE Security & privacy*, vol. 1, no. 3, pp. 75–79, 2003.

[23] E. Sun and N. H. Hassan, "Cybercrime incident reporting system," in *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, IEEE, 2022, pp. 1–5.

[24] S. van de Weijer, R. Leukfeldt, and S. Van der Zee, "Reporting cybercrime victimization: Determinants, motives, and previous experiences," *Policing: An International Journal*, vol. 43, no. 1, pp. 17–34, 2020.

[25] S. Aairam, K. Kumar, and J. Singh, "Cyber crime reporting system," *International Journal of Computer Science and Information Technologies*, vol. 11, no. 2, pp. 45–50, 2020. [Online]. Available: https://ijcsi.org/papers/IJCSI-11-2-45-50.pdf.

[26] C. Breen, C. Herley, and E. Redmiles, "A large-scale measurement of cybercrime against individuals," Apr. 2022, pp. 1–41. DOI: 10.1145/3491102.3517613.

[27] Y. M. Jadhav, "Analyzing efficacy and enhancing accessibility: A study of india's national cyber crime reporting portal in addressing financial cybercrimes," 2024.

[28] M. Babar, P. Sahare, R. Katre, P. Ganvir, B. Sakharwade, and R. Chikate, "Research on online crime server and management," 2021.

[29] D. Puchalski, A. Smith, and L. Zhang, "Trustworthy ai-based cyber-attack detector for network cyber crime forensics," in *19th International Conference on Availability, Reliability and Security (ARES)*, IEEE, 2024. DOI: 10.1109/ARES.2024.9912345. [Online]. Available: https://ieeexplore.ieee.org/document/9912345.

[30] M. N. Rita and F. B. Shava, "Chatbot driven web-based platform for online safety and sexual exploitation awareness and reporting in namibia," in *2021 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, IEEE, 2021, pp. 1–5.

[31] M. Khairy, T. M. Mahmoud, T. Abd-El-Hafeez, and A. Mahfouz, "User awareness of privacy, reporting system and cyberbullying on facebook," in *Advanced machine learning technologies and applications: Proceedings of AMLTA 2021*, Springer, 2021, pp. 613–625.

[32] D. Murtezaj, "Public security user interfaces: Promoting cybersecurity behavior through human-centered design," in *Proceedings of the 2024 New Security Paradigms Workshop*, ACM, 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/3703465.3703470.

[33] D. R. Jacobs, "Unraveling the real-world impacts of cyber incidents on user behavior," *HCI for Cybersecurity, Privacy and Trust: 6th International Conference, HCI-CPT 2024*, 2024. DOI: 10.1145/3743014.3743121. [Online]. Available: https://dl.acm.org/doi/10.1145/3743014.3743121.

[34] Elsevier, "Design principles for cognitively accessible cybersecurity training," *Computers & Security*, 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404823005400.

[35] S. G. Correia, "Making the most of cybercrime and fraud crime report data: A case study of uk action fraud," *International Journal of Population Data Science*, vol. 7, no. 1, 2022.

[36] H. S. Lallie et al., "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & security*, vol. 105, p. 102 248, 2021.

[37] M. Nouh, J. R. Nurse, H. Webb, and M. Goldsmith, "Cybercrime investigators are users too! understanding the socio-technical challenges faced by law enforcement," *arXiv preprint arXiv:1902.06961*, 2019.

[38] C. Leuprecht, D. B. Skillicorn, and V. E. Tait, "Beyond the castle model of cyber-risk and cyber-security," *Government Information Quarterly*, vol. 33, no. 2, pp. 250–257, 2016.

[39] M. Bidgoli and J. Grossklags, "End user cybercrime reporting: What we know and what we can do to improve it," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, IEEE, 2016, pp. 1–6.

[40] A. B. Sakpere, A. V. Kayem, and T. Ndlovu, "A usable and secure crime reporting system for technology resource constrained context," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, IEEE, 2015, pp. 424–429.

[41] M. Bidgoli, B. P. Knijnenburg, J. Grossklags, and B. Wardman, "Report now. report effectively. conceptualizing the industry practice for cybercrime reporting," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, 2019, pp. 1–10.

[42] Springer-Verlag, "Interdependencies, conflicts and trade-offs between security and usability: Why and how should we engineer them?" In *Lecture Notes in Computer Science*, vol. 11594, Springer, 2019. DOI: 10.1007/978-3-030-22351-9_21. [Online]. Available: https://link.springer.com/10.1007/978-3-030-22351-9_21.

[43] M. Hassenzahl and N. Tractinsky, "User experience - a research agenda," *Behaviour Information Technology*, vol. 25, no. 2, pp. 91–997, 2006. DOI: 10.1080/01449290500330331.

[44] M. A. Blythe, *Funology: From usability to enjoyment*, 2004.

[45] M. Maguire and P. Isherwood, "A comparison of user testing and heuristic evaluation methods for identifying website usability problems," in *Design, User Experience, and Usability: Theory and Practice: 7th International Conference, DUXU 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part I 7*, Springer, 2018, pp. 429–438.

[46] L. Hasan, "The usefulness of user testing methods in identifying problems on university websites," *JISTEM-Journal of Information Systems and Technology Management*, vol. 11, pp. 229–256, 2014.

[47] S. E. Rosenbaum, C. Glenton, and J. Cracknell, "User experiences of evidence-based online resources for health professionals: User testing of the cochrane library," *BMC Medical Informatics and Decision Making*, vol. 8, no. 1, p. 34, 2008. DOI: 10.1186/1472-6947-8-34. [Online]. Available: https://bmcinformdecismak.biomedcentral.com/articles/10.1186/1472-6947-8-34.

[48] T. P. Thyvalikakath, V. Monaco, H. Thambuganipalle, and T. Schleyer, "Comparative study of heuristic evaluation and usability testing methods," in *Studies in Health Technology and Informatics*, vol. 143, 2009, pp. 322–327. DOI: 10.3233/978-1-58603-979-0-322.

[49] R. Khajouei, S. H. Gohari, and M. Mirzaee, "Comparison of two heuristic evaluation methods for evaluating the usability of health information systems," *Journal of Biomedical Informatics*, vol. 80, pp. 37–42, 2018. DOI: 10.1016/j.jbi.2018.02.016.

[50] M. Umar, M. U. Bakhat, and M. Hassan, "Mapping hci principles to evaluate the usability of learning applications for cci user," *International Journal of Computer Science and Telecommunications*, vol. 11, no. 2, pp. 1–7, 2020, available from IJCS&T, March 2020 issue. [Online]. Available: https://www.ijcst.org/Volume11/Issue2/p1_11_2.pdf.

[51] J. W. Creswell, "Steps in conducting a scholarly mixed methods study," 2013.

[52] H. Kallio, A.-M. Pietilä, M. Johnson, and M. Kangasniemi, "Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide," *Journal of advanced nursing*, vol. 72, no. 12, pp. 2954–2965, 2016.

[53] Pivotal Software, *Spring boot reference documentation*, Retrieved from https://spring.io/projects/spring-boot, 2020. [Online]. Available: https://spring.io/projects/spring-boot.

[54] M. Stonebraker and G. Kemnitz, "The postgres next-generation database management system," *Communications of the ACM*, vol. 34, no. 10, pp. 78–92, 1991.

[55] D. Merkel, "Docker: Lightweight linux containers for consistent development and deployment," *Linux Journal*, no. 239, 2014.

[56] Facebook, *React – a javascript library for building user interfaces*, Retrieved from https://react.dev, 2013. [Online]. Available: https://react.dev.

[57] J. R. Lewis, "The system usability scale: Past, present, and future," *International Journal of Human–Computer Interaction*, vol. 34, no. 7, pp. 577–590, 2018. DOI: 10.1080/10447318.2018.1455307.

[58] S. McLellan, A. Muddimer, and S. C. Peres, "The effect of experience on system usability scale ratings," *Journal of Usability Studies*, vol. 7, no. 2, pp. 56–67, Feb. 2012.

[59] T. Franke, C. Attig, and D. Wessel, "A personal disposition for technology interaction: Development and validation of the affinity for technology interaction (ati) scale," *International Journal of Human–Computer Interaction*, vol. 35, no. 6, pp. 456–467, 2018. DOI: 10.1080/10447318.2018.1456150.

[60] M. Henrich, M. W. Kleespies, P. W. Dierkes, and S. Formella-Zimmermann, "Inclusion of technology affinity in self scale – development and evaluation of a single item measurement instrument for technology affinity," *Frontiers in Education*, vol. 7, p. 970 212, 2022. DOI: 10.3389/feduc.2022.970212.

[61] M. W. B. Shadat, M. S. Islam, I. Zahan, and M. Matin, "Digital literacy of rural households in bangladesh," 2020.

[62] K. Hernandez and T. Roberts, "Leaving no one behind in a digital world," *K4D Emerging Issues Report. Brighton, UK: Institute of Development Studies*, 2018.

[63] M. Hibbeln, J. L. Jenkins, C. Schneider, J. S. Valacich, and M. Weinmann, "How is your user feeling? inferring emotion through human–computer interaction devices," *Mis Quarterly*, vol. 41, no. 1, pp. 1–22, 2017.

[64] L. Irani, J. Vertesi, P. Dourish, K. Philip, and R. E. Grinter, "Postcolonial computing: A lens on design and development," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2010, pp. 1311–1320.

[65] V. K. Cannanure et al., "Decolonizing hci across borders," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–5.

[66] S. A. RAHMAN, "Exploring and analyzing the design methodologies for developing multi-channel e-government websites: Towards improving the usability of e-government websites of bangladesh," Ph.D. dissertation, DEPARTMENT OF COMPUTER SCIENCE and ENGINEERING, 2020.

[67] A. Sattar, N. Khan, M. Moheeuddin, and N. U. K. Shaon, "Bridging the gap in hci between industry and academia: A perspective in bangladesh," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, 2019, pp. 1–6.

[68] L. Pimentel, M. d. R. Bernardo, and T. Rocha, "The implementation of public chatbots to raise awareness of computer crime," *International Journal of Human–Computer Interaction*, pp. 1–23, 2025.

[69] W. Fallatah, "The influence of usable security on security culture," Ph.D. dissertation, University of Nottingham, 2025.

Appendix 1

Questions for First User Testing

Demographic Questions

- Name
- Age
- Gender
- Occupation/ Field of study

Behavioural/ Perception Questions

- What does the user know about cybercrime?
- Have they ever tried reporting cybercrime before? If yes, where?

During Task

- Explore the following websites: CID, BTRC, and DSA
- Explore this mobile application: Online GD application

Experience

- Share your whole experience.

Problems Faced as a Tech User

- What types of issues did you face during exploration?

Suggestions

- Share your opinions and suggestions from your side.
- Positive feedback
- Negative feedback

Appendix 2

Semi-Structured Interview of Officials

Demographics

- What is your age?
- What is your role/title, and which organization/unit do you work in?
- Where is your primary work location (thana/division), and is it mainly urban or rural?
- Which reporting tools do you primarily use (e.g., web form, 999, social media inbox, internal app)?

Core Questions

Entry points & awareness

- How do citizens usually find and start a cyber complaint (in-person, 999, website, social media)? Who struggles the most to find the right place?

Intake flow

- Please walk me through the steps from first contact to case assignment. Where do delays or drop-offs happen?

Information quality

- What information is often missing at intake (e.g., IDs, evidence, links) that slows routing or action?

Usability of current platforms

- What works well vs. poorly in the current reporting websites/apps (navigation, form labels, help text, evidence upload, language support)?

Verification & abuse control

- How is identity verified now (e.g., NID/birth certificate)? What breaks in practice? How do you screen fake/low-quality reports?

Status & feedback

- Can citizens track their case status today? What would a clear, useful status page or notification look like?

Capacity & tools

- What resource or access limits (people, training, system access, API caps) block timely triage and investigation?

Cross-agency coordination

- Where do hand-offs with social media, mobile operators, or banks stall? What one change would fix most delays?

Policy & hosting

- What policy constraints (e.g., online GD scope) or hosting/governance needs (local cloud, audit trails, role-based access) matter most?

Top improvements

- If you could change only three things in the reporting ecosystem, what would they be—and why?

Probing Questions

- "Can you give a recent example of this going well—and one that failed?"
- "Which exact screen/step causes confusion or rework?"
- "What validation or auto-check would prevent that error at submission time?"
- "What single metric or dashboard would help you triage faster?"
- "What standardized form would remove most back-and-forth with platforms?"

Open-Ended Closers

- "Is there anything important we didn't ask that would improve the citizen and officer experience?"
- "If you could leave one message for the designers/policymakers of the next platform, what would it be?"

Appendix 3

Questions For Users

Demographic Questions

- Name
- Age
- Gender
- Occupation/ Field of study

Behavioural/ Perception Questions

- What does the user know about cybercrime?
- Have they ever tried reporting cybercrime before? If yes, where?
- How confident do they feel using government websites?

During Task (Think-Aloud Prompts)

- What do they expect to happen when they click a particular feature?
- Is there any confusion using the features?
- What do they think of specific buttons?

After Each Task

- Was this task easy or difficult? (Likert scale: 1 = very difficult, 5 = very easy)
- How long do they think it took? (faster/slower than expected)
- What would you change to make it easier?
- Etc. according to need.

Post-Test Questionnaire

A post-test questionnaire is a short survey that participants complete after finishing all the usability test tasks on the website. It captures users' overall impressions (not just about one task). It helps you measure usability, satisfaction, and trust in the system. It is often a mix of rating-scale questions (quantitative) and open-ended questions (qualitative). Adapted from System Usability Scale (SUS) + your features.
Responses: Strongly Disagree: 1, Disagree: 2, Neutral: 3, Agree: 4, Strongly Agree: 5

1. I found the website easy to use.
2. The registration and login process was straightforward.
3. I felt confident submitting a cybercrime report.
4. The report tracking system was clear and useful.
5. The chatbot was helpful in answering my questions.
6. The "Types of Fraud" section improved my understanding.
7. The news section, Contact Us and About sections were relevant and easy to navigate.
8. Receiving a confirmation email made me feel reassured.
9. I would use this platform again to report a cybercrime.
10. I would recommend this website to others.
11. Report form is easy to understand.
12. The feedback section is useful.
13. Etc. according to your need.

Open-Ended Questions

- What did you like most about the website?
- What frustrated you the most?
- Did you find anything missing?
- Was there any feature that surprised you (good or bad)?
- Did you find anything missing that you expected?
- If you could improve one part of the system, what would it be?
- Do you have suggestions to improve the system?
- Share your experience on our website.
- Etc. according to your need.

SUS (System Usability Scale) Questionnaire

Scale: 1 — Strongly Disagree, 2 — Disagree, 3 — Neutral, 4 — Agree, 5 — Strongly Agree

No.	Question
1	I think that I would like to use this system frequently.
2	I found the system unnecessarily complex.
3	I thought the system was easy to use.
4	I think that I would need the support of a technical person to be able to use this system.
5	I found the various functions in the system were well integrated.
6	I thought there was too much inconsistency in this system.
7	I imagine that most people would learn to use this system very quickly.
8	I found the system very cumbersome to use.
9	I felt very confident using the system.
10	I needed to learn a lot of things before I could get going with this system.

ATI (Affinity for Technology Interaction) Questionnaire

Scale Options: 1 — completely disagree, 2 — largely disagree, 3 — slightly disagree, 4 — slightly agree, 5 — largely agree, 6 — completely agree

No.	Question
1	I like to occupy myself in greater detail with technical systems.
2	I like testing the functions of new technical systems.
3	I predominantly deal with technical systems because I have to.
4	When I have a new technical system in front of me, I try it out intensively.
5	I enjoy spending time becoming acquainted with a new technical system.
6	It is enough for me that a technical system works; I don't care how or why.
7	I try to understand how a technical system exactly works.
8	It is enough for me to know the basic functions of a technical system.
9	I try to make full use of the capabilities of a technical system.