

Cyber Threats and Scams in FinTech Organizations: A brief
overview of financial fraud cases, future challenges, and
recommended solutions in Bangladesh

by

Md. Jafrin Hossain
22141066

Rejuan Haque Rifat
18301283

Mahadi Hasan Mugdho
18301258

Mohona Jahan
18301101

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
May 2022

© 2022. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis that we have provided is the result of our distinct individual research conducted while studying at Brac University.
2. The thesis does not include anything that has been previously published or authored by a third party, unless it is properly cited with complete and correct referencing.
3. The thesis does not include any material that has been approved or submitted for any other university or even other institution's diploma or degree.
4. We have acknowledged all significant sources of assistance.

Student's Full Name & Signature:



Md. Jafrin Hossain
22141066



Rejuan Haque Rifat
18301283



Mahadi Hasan Mugdho
18301258



Mohona Jahan
18301101

Approval

The thesis titled “Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh” submitted by-

1. Md. Jafrin Hossain(22141066)
2. Rejuan Haque Rifat(18301283)
3. Mahadi Hasan Mugdho(18301258)
4. Mohona Jahan(18301101)

Of Spring, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on May, 2022.

Examining Committee:

Supervisor:
(Member)

Annajiat Alim Rasel
Senior Lecturer
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

M. Abdur Rahman Adnan
Visiting Faculty
Department of Computer Science and Engineering
Brac University

Thesis Coordinator: (Member)

Md. Golam Rabiul Alam, PhD
Associate 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

The idea of financial systems has changed with the touch of applications based on information technology and came up with a new terminology called ‘FinTech’ (Financial Technology). With the rising technology, Fintech has become a modern phenomenon. Financial organizations deal with highly confidential and sensitive information, including personal and financial data, all of which are the primary target of the cybercriminal. As users and other stakeholders are massive in number, and many are not concerned about security, they often find themselves victims. In the perspective of Bangladesh, most of the attacks on the fintech industry are generated using social engineering methods. The sole purpose of the study is to find good practices and recommendations for ensuring the security and privacy of user data in the financial technology industry since FinTech applications and services carry a lot of sensitive data of its users. This research study aims to provide an extensive set of recommendations to secure FinTech services. FinTech service-providing organizations may consider adopting these recommended policies to secure their business and the users of its services. It provides a detailed analysis of existing security problems, detection techniques, and security solutions available for FinTech. Finally, it discusses future challenges to ensuring financial technology applications’ security and privacy.

Keywords: Cyber Security; FinTech; Cyber Threat; Finalcial Scam; MFS; Cyber Attack; Social Engineering; Blockchain; Hyperledger Fabric; Framework; Prediction; Prevention

Acknowledgement

First and foremost, we express gratitude to The almighty ALLAH for allowing us to complete our thesis without any major setbacks.

Secondly, we would like to convey our sincere gratitude to our inspirational thesis supervisor Mr. Annajiat Alim Rasel and co-supervisor Mr. Abdur Rahman Adnan, for their valuable time and guidance.

Finally, we may be unable to accomplish our ambitions without our parents' continuous support. We are on the verge of graduating because of their unwavering support and prayers.

Table of Contents

Declaration	i
Approval	ii
Abstract	iv
Acknowledgment	v
Table of Contents	vi
List of Figures	ix
List of Tables	xi
Nomenclature	xiv
1 Introduction	1
1.1 Research Problem	2
1.2 Research Objective	3
2 Literature Review	5
2.1 Fintech	5
2.2 Cybersecurity	6
2.3 Related Works	6
3 Research Activities	10
3.1 Methodology	12
4 Data Description	13
4.1 Problem Framing	13
4.2 Data Collection	13
4.2.1 Collecting Raw Data	13
4.2.2 Global Data	13
4.2.3 Domestic Data	13
4.2.4 Primary Data	14
4.2.5 Data from Survey	14
4.2.6 Secondary Data	14
4.3 Datasets	14
4.3.1 PaySim Synthetic Financial Dataset	14
4.3.2 BankSim Dataset	14

4.3.3	Socradar Dataset from Deep Web	14
4.3.4	Other Datasets	15
4.4	Data Processing	15
4.4.1	Editing of Data	15
4.4.2	Coding of Data	15
4.4.3	Classification of Data	15
4.4.4	Tabulation of Data	15
4.4.5	Data Diagrams	15
4.5	ML Model	15
4.5.1	Extreme Gradient-Boosted (XGBoost) Algorithm	16
4.6	Web Scraping using BeautifulSoup	16
4.7	In-depth Data Analysis	17
4.7.1	Inferential Analysis	17
4.7.2	Predictive Analysis	17
4.7.3	Qualitative Analysis	17
4.7.4	Hypothetical Analysis	17
4.7.5	Interpreting the Results	17
4.8	Data Storage	17
5	Analysis and Findings	18
5.1	Based on PaySim Synthetic Financial Dataset	18
5.2	In-depth Analysis	19
5.3	Based on Deep Web Dataset	20
5.3.1	Attack Types	20
6	Cyberattacks in Broader Categories	25
6.1	In terms of Bangladesh	26
6.2	Affected Countries	26
6.3	State-Backed Hackers	27
6.4	Attacks on Different Financial Activities	28
6.5	In terms of Gender	29
7	Cyberattacks in Bangladesh	30
7.1	Attacks on Financial Zones in Bangladesh	31
7.2	Cyberattacks on Different Geographic Areas in Bangladesh	31
7.3	Cyberattacks on Mobile Banking in Different Geographic Areas in Bangladesh	32
7.4	Attacks on Mobile Banking in Bangladesh	33
8	Result and Discussion	34
9	Solutions	36
9.1	Existing Solutions	36
9.2	Proposed Framework	41
9.2.1	Short Description of FinSec Framework	41
9.3	Action Unit	42
9.3.1	Human Factors	42
9.3.2	Securing Human Factors	43
9.3.3	End-User Training Model	47

9.4	Digital Infrastructures	48
9.4.1	Securing Digital Factors	48
9.4.2	Hyperledger Fabric	52
9.4.3	Hybrid Cloud	53
9.5	Physical Infrastructures	54
9.5.1	Securing Physical Factors	54
9.6	Knowledge Unit	55
9.6.1	Potential Threats Study	55
9.6.2	Upgrade and Update	55
9.7	Simulation Unit	55
9.7.1	Attacks Simulation	56
9.7.2	Forensic Analysis	56
10	Implementation	57
10.1	Analysis	58
11	Comparison	64
12	Drawbacks	66
13	Future Work	67
14	Conclusion	68
	Bibliography	73
	Appendix	74

List of Figures

3.1	Research Activities	11
3.2	Methodology	12
4.1	Output of XGBoost; Source: towardsdatascience.com	16
4.2	Web scrapping using BeautifulSoup	16
5.1	An instance of PaySim Dataset	18
5.2	Different Types of Transactions	18
5.3	Fraud Distributions	19
5.4	Transactions Over Time	19
5.5	Transactions Over Amount	20
5.6	Common Cyberattacks	24
6.1	Cyberattacks in Broader Categories	25
6.2	Cyber-attacks in Bangladesh	26
6.3	Countries affected by massive cyberattacks more than 10 times	26
6.4	State Backed Hackers	27
6.5	Targeted Countries	27
6.6	Nationality of Cyberattacks Conducting Groups	28
6.7	Attacks on different financial activities	29
6.8	Classification in the context of gender	29
7.1	Cyberattacks in Bangladesh	30
7.2	Attacks on financial zones in Bangladesh	31
7.3	Cyberattacks in different geographic areas in Bangladesh	32
7.4	Cyberattacks (MFS) in different geographic areas in Bangladesh	32
7.5	Attacks on Mobile Banking in Bangladesh	33
9.1	Proposed “FinSec Framewok”	41
9.2	End-User Traning Model	47
9.3	3WA Auth	48
9.4	A renowned MFS’s Reference	49
9.5	Security Question	49
9.6	Security Questions of a renowned bank	50
9.7	A renowned MFS’s payment via SSLCommerz (OTP)	50
9.8	A renowned MFS’s payment via (Pin code)	51
9.9	Gamification to pass 3WA	51
9.10	Example of proposed operation-based OTP text	52
9.11	Hyperledger Fabric Architecture; Source: jktech.com	53

9.12 Hybrid Cloud with Hyperledger Fabric (Edited from IBM Documentation	54
9.13 Proposed Security Team	56

List of Tables

5.1	The most common attack types that occurred all over the world . . .	20
5.2	The most common attack types that occurred all over the world . . .	21
5.3	The most common attack types that occurred all over the world . . .	22
5.4	The most common attack types that occurred all over the world . . .	23
10.1	Preventing Attacks	58
10.2	Preventing Attacks	59
10.3	Preventing Attacks	60
10.4	Preventing Attacks	61
10.5	Preventing Attacks	62
10.6	Preventing Attacks	63
11.1	Framework Comparison	64
11.2	Framework Comparison	65

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

3WA Three-Way Authentication

ACPS Automated Contract Preparation System

ADPM Anti-Counterfeit Deterministic Prediction Model

AML Anti-Money Laundering

API Application Programming Interface

AR Augmented Reality

ARP Address Resolution Protocol

ATM Automated Teller Machine

AWS Amazon Web Services

BCT Blockchain Technology

BGDe – GOVCIRT Bangladesh Government's Computer Incident Response Team

BOT Build Operate Transfer

CA Certificate Authority

CNBC Consumer News and Business Channel

DDOS Distributed Denial of Service

DFS Digital Financial Services

DHCP Dynamic Host Configuration Protocol

DLP Data Leakage Prevention

DLT Distributed Ledger Technology

DNS Domain Name System

DoS Denial-of-Service

EFTN Electronic Fund Transfer Network

FinTech Financial Technology
GCP Gross Corporate Product
HKMA The Hong Kong Monetary Authority
HSM Hardware Security Module
HTTP Hypertext Transfer Protocol Secure
HTTFS Anti-Money Laundering
IBM International Business Machines Corporation
ICT Information and Communication Technology
IFC International Finance Corporation
IoT Anti-Money Laundering
IP Internet Protocol
IPS/IDS Intrusion Prevision and Intrusion Detection Solutions
IT Information Technology
KYC Know Your Customer
LAN Local Area Network
LC Letter of Credit
M – PAA Monte Carlo Model-Based Prediction Analysis Algorithm
MAC Media Access Control
MBPS Mobile Banking Payment System
MFA Multi-factor Authentication
MFS Mobile Financial Services
MitM Man in the Middle
ML Machine Learning
MQ Message Queue
NAC Network Access Control
NFC Near Field Communication
NGFW Next-Generation Firewall
NGIPS Next-Generation Intrusion Prevention System
NIST National Institute of Standards and Technology

OTP One-time password

PEU Perceived Ease of Use

PIN Personal Identification Number

PKI Public Key Infrastructure

PUP Potentially Unwanted Program

RAT Remote Access Trojan

RDP Remote Desktop Protocol

RS Regulatory Sandbox

RSA Rate-Sensitive Assets

SIEM Security Incident and Event Management

SMS Short Messaging Service

SOC Security Operation Centre

SPIM Spam Sent via Instant Message

SQL Structured Query Language

SRESOFL Security Requirement Engineering with Structured
Object-Oriented Formal Language

SSL Secure Sockets Layer

STP Spanning Tree Protocol

SWIFT The Society for Worldwide Interbank Financial Telecommunications

TAM Technology Acceptance Model

URL Uniform Resource Locator

USSD Unstructured Supplementary Service Data

VR Virtual Reality

WAF Web Application Firewall

WiFi Wireless Fidelity

Chapter 1

Introduction

It is hard to envisage a nation or territory without sovereignty, protecting civilians from external and internal threats and attacks. If we consider the internet world a global region, there should have protectors to save its users from malicious threats and attacks. According to Marshall McLuhan, this region is a “Global Village” based on digitalized data communication[1]. The basic building block of today’s worldwide data communication system is the Internet’s invention, which made it feasible[2]. All services are reliant on computer systems because of their efficiency and correctness.

Even while the widespread usage of computerized systems makes life simpler and quicker in every way, people underestimate the system’s security. Consequently, bad actors with technical expertise are always looking for flaws in a system to get unethical access to private data, harm the system, and even steal the funds of one’s account.

Surprisingly, the success rate for stealing money from a user’s account constantly rises. The more frightening concern is that cybercrime actors are not satisfied with targeting just one person. They are, however, targeting businesses, banks, and even reserve funds.

When it comes to Bangladesh has experienced one of the biggest heists globally, losing almost a billion-dollar from the country’s reserve bank in 2016[49]. After about a few years, the nation was hit by a cyber-attack that targeted 200 organizations in 2021[48]. Nevertheless, that was not the original case that made the country attractive to international hackers to attack the banking sector. Studying the Internet and mobile banking history in Bangladesh is vital to get the attackers’ motive for choosing the country for such massive cyber-attacks. In late 2011, a pioneer private bank, BRAC, introduced the country’s first mobile financial service, which attracted massive users within a short period. However, scammers randomly targeted bKash users and got the massive success that 10-12 incidents of extortion via bKash were recorded every day, according to a top Rab officer[5]. In 2021, so many mobile financial services were introduced, and the cases rose so high that they could find them accurately.

Moreover, people from all classes, races, and religions are related to today’s digital financial system. Thus, the loss of the attacks directly hit the financial condition of

the victim. Even in a broader sense, its impact on the economy is alarming. Thus, the security concern of the industry is one of the most considerable matters in the country nowadays.

The study emphasizes every aspect from the end user's perspective to top industrial infrastructure to find the best cyber-attack prevention. The research reflects that even a single mistake can open the door for attackers who may create substantial financial damage. It shows a framework for both individuals and organizations. The framework guides both precautions and responses to the bad actors. So, in this era of the Internet and technology, cyber-attacks and bad actors can be dealt with by following the framework and keeping a security-centric mindset.

1.1 Research Problem

Problem to be researched attacks against cyber security are becoming more common as technology overgrows. According to the author [(Nilufa Khatun, 2021)], the number of people registered in mobile banking at the beginning of 2020 was 80.90 million. In Bangladesh, it increased and became 90.57 million by July 2020, during the lockdown[58]. Having such a massive increase in the number of users by 2020, millions of taka are regularly exchanged through mobile banking. It is essential to protect such online transactions over the Internet, keeping concerned.

We looked at various studies that discussed security and privacy difficulties and issues for our study. According to [(Iñaki Aldasoro, 14 January 2021)], Cyber security is becoming more critical as the economy and financial system become increasingly digitized[45]. Hackers are salivating at the prospect of stealing money as customers flock to the fintech industry. People here utilize the mobile banking system, and many of them are first-time users concerned with this new technology. Fintechs, particularly mobile banking organizations (Bkash, Rocket, Nagad), warn their customers not to disclose their passwords, OTP (one-time passwords), or other sensitive information. On the other hand, social engineering is the first and most fundamental stage in hacking, and Hackers utilize it to acquire personal information from individuals in this way.

Furthermore, many users are illiterate, and hackers may influence them and obtain their information due to their lack of education. On the contrary, many fintech industry professionals who interact directly with end-users, known as "Agents," are under-trained, impacting end-users since they cannot assist them adequately due to their lack of it.

Because of the rising number of financial institutions worldwide, many attacks need specialized equipment and planning, and new types of Ransomware, Phishing, and Malware attacks emerge regularly. According to [3 (PEACE, n.d.)], seventeen new attacks occurred along with the previous type of procedure[67]. In 2016, hackers with ties to North Korea breached Bangladesh Bank's servers and utilized the SWIFT network to send fake money transfer instructions (Bangladesh Bank, 2019)[50]. The event drew attention to the increasing cyber vulnerabilities faced by payment networks and related infrastructures.

Financial institutions, like other firms, have temporarily switched to remote work to protect their personnel during the Covid-19. As the majority of operations transition to the digital environment, cyberattacks may become more prevalent. In December 2020 (KrebsOnSecurity, 2020), it was by thousands of businesses and government organizations worldwide[40]. As employees work from home utilizing corporate and personal devices and networks, new risks may emerge, such as several family members connecting to the very same network and perhaps compromising devices to malware that could infect the business environment.

Bangladesh is lagging in utilizing technology to automate and digitalize financial transactions despite its expanding market. According to the Worldwide Fintech Index 2021 (Tributr, 2021), even though Bangladesh's fintech ecosystem has been expanding — and is likely to continue to grow in the future years — the country appears to be trailing behind its global peers[47]. Bangladesh was placed 78th out of 83 nations in the report, suggesting lagging in adopting technology to automate and digitalize financial transactions.

Consequently, according to the state-run Bangladesh e-Government Computer Incident Response Team which is under the Ministry of Posts, Telecommunications and Information Technology (Express F., 2021), the lack of specific simulated standards and structure for the fintech organization is allowing this type of attack to occur[37]. Furthermore, consumers and employees directly involved in this do not sufficiently understand how to utilize this digital platform and ensure its security correctly.

1.2 Research Objective

In both public and private sectors, obtaining money for network security initiatives has proven to be challenging. Quantifying the business effectiveness of information confidentiality to a firm is highly challenging. Typically, management recognizes the importance of investing in cybersecurity only when a data security breach directly impacts a company's reputation.

Associations emphasize defending their data security from potential hackers rather than having breaches occur from inside the business through their employees, necessitating research into the subject. Local and global business professionals could be decided to make keenly aware of a diverse array of vulnerabilities. Fintech companies allow consumers and businesses to move money, manage investments, and access online lending and personal financial resources. As a result, Fintech companies are a prime target for cybercriminals.

To build a secure cyber network across the country, promote faith and credibility in IT infrastructure and cyberspace operations, and enhance IT engagement throughout the industry.

Develop an assessment structure to formulate access controls and marketing and support strategies for adherence to international security guidelines and principles as part of the accredited certification (product, process, technology people).

The guidelines must be emphasized in terms of ensuring a sustainable internet atmosphere.

To increase the visibility of the integrity of ICT products and services by providing infrastructure for security testing and certification.

Appropriate legislative action enables effective cybercrime detection, prosecution, and the improvement of law enforcement capacities.

To provide information protection during the processing, management, preservation, and transit of data to protect citizen privacy and reduce financial damage due to cybercrime and data breaches.

To promote the purpose of cyber security by improving civic engagement by building general knowledge and utilizing relationships.

To accomplish a protected, trustworthy internet layer storage platform for the entire company and approved intermediaries, with the certainty that the environment can utilize confidential material.

To offer a comprehensive, robust framework that can secure end-users and organizations from any cyber-attacks targeted at the fintech industry.

Chapter 2

Literature Review

Nowadays, the thought of banking frameworks has changed with this revolution of Fintech. Furthermore, with the growth of technology, anyone can send money or make payments anywhere with a few clicks. Nevertheless, the fact is that most of the end-users are not concerned about the security of her personal and financial data. However, people with a good understanding of the technologies, usually known as 'Hackers', use this unconsciousness of the end-users and make them fall into their traps. As a result, they stole the credentials and easily transferred funds from victims to their accounts.

On the other hand, end-users and people from financial organizations also find themselves in the loophole of hackers' trap because of their simple mistakes of not being enough concerned. However, weak infrastructure also leads to dangerous cyberattacks by expert hackers. Again, a developing country like Bangladesh, where Fintech was introduced in recent years, has already faced massive cyber-attacks in the history of the world. In terms of mobile banking, everyday people from different parts of the country face scamming and losing funds from mobile banking service providers such as Bkash, Nagad, and rocket. So, it is a must to know at least some of the basic ideas of the attacks that can take place in this sector to make safe transactions of funds for everyone, including employees, stakeholders, and end-users related to the Fintech industry.

2.1 Fintech

Fintech can be described as integrating technology to automate and improve all the services offered by Financial Services Companies, including typical banks, cashless service providers, mobile financial services, and e-money services, making it easier and faster to use daily end-users. Within the late 19th century, two distinct fields, finance, and technology, combined to deliver the introductory period of financial globalization. After breaking the seed level of the fintech industry, the start-up which became the most successful one in this vast potential field of Fintech was known as PayPal[61]. Today, in 2021, according to Forbes, in terms of online payments, PayPal is one of the biggest service providers having more than 377 million users, generating almost 15.4 billion transaction costs of \$1 trillion payment volume.

In the context of Bangladesh, people were introduced to Fintech vastly by a growing venture of BRAC, bKash Limited, back in 2011. According to International Finance Corporation (IFC), it has more than 23 million active users and conducts around 110 million transactions every month[5]. The success of bKash inspired other giant companies to come up with their offerings to compete with Bkash. Hence, the people of Bangladesh have seen other ventures like Nagad, Rocket, Sure-Cash, and Upay.

Because of having very little knowledge of cyber threats, end-users face many scammers and frauds nowhere and then. As a result, the rate of being scammed is seriously getting higher every day. In response, industry stakeholders are not taking the necessary steps to train the end-users and employees.

2.2 Cybersecurity

According to Burley (2017), cybersecurity refers to:

An interdisciplinary course of study, including law, policy, human factors, ethics, and risk management[16].

In other words, Seemma Sundaresan, Nandhini M, Sowmiya. (2018) portrait cybersecurity as:

In a computing context, security comprises enterprises that use cyber security and physical security to save against unauthorized access to the data center and other computerized systems. Security, designed to maintain confidentiality, integrity, and data availability, is a subset of cyber security[28].

To keep the fintech industry safe from frauds,scammers and hackers, every single organization related to this industry needs to have a strong backbone of cybersecurity to prevent their end-users from fraud transactions of funds.

2.3 Related Works

This specific portion of the study reflects the previous research on the relevant field and how the researcher responded to the cyberattacks. This research determines to get a brief idea of every possible solution more efficiently. Thus, it is not bound to a geographical place; instead, it determines to gather ideas from different parts of the world.

The framework Security Requirement Engineering with Structured Object-Oriented Formal Language was proposed by B. O. Emeka and S. Liu (SRESOFL)[19]. The framework includes Semi-Formal Specifications, Formal Specifications, and Application codes in a three-step evolutionary approach. The core concept of the framework is to recognize the attack's surface and switch between several data flows in response to the attacks.

In another study, D. Kriz proposed six principles to improve the total cyberworld. According to him, public-private partnerships should leverage, reflecting a global

cyber environment. Furthermore, organizations should respond to newer threats fastly. He concluded by focusing directly on attackers[4].

C. Mockel and A. E. Abdallah created new information security risk management methodologies and tools to improve the security of e-banking systems[3]. The main suggestion was to implement security concerns to the developers and IT persons developing banking-related applications. They proposed an alternative way of data flow diagram different from regular ones to ensure more protection.

In 2019, Jason Goldberg, a Barclays analyst, appeared on CNBC's "Power Lunch" and stated that the leading banking technology dangers include malware, unprotected data, and unsafe third-party service[51]. Cybersecurity risks are defined by Upguard, the ready-made platform for protecting your institution's confidential documents, as a series of fraudulent acts aimed at compromising or stealing data and disrupting the bank's electronic existence as a whole. The financial system must cope with increasing risks daily since they affect clients' resources and reputations and force banks to regain data regularly, resulting in significant financial outlays. This makes it easier for hackers to access sensitive data, making redundant data one of the most severe bank cybersecurity dangers.

According to Prabhu, FinTech, or digital banking, has been the financial sector's most significant game-changer, affecting banking, public liability, transactions, and asset allocation. The expansion of Fintech, on the other hand, represents a significantly more significant potential threat to the banking sector, considering the volume of efficient and high data stored inside it[60].

As a result, planning is an essential aspect of Fintech, with each company having its list of requirements. Therefore, because fintech companies have a collection of large amounts of confidentiality, including complete contact information, network security is one of their key objectives.

In another study, Arash Habibi Lashkari claims that FinTech is a broad term that refers to various technical tactics that have boosted the capabilities of existing economic assets or allowed the creation of new fintech alternatives[56].

This contains traversing vulnerabilities, detecting security flaws, mitigating risks, and developing constructive management systems, guidelines, and infrastructures, further allowing the layout of an adequate security foundation for FinTech used by banking institutions to assist.

In 2014, M. Lagazio, N. Sherif, and M. Cushman proposed a multi-level model based on a system dynamics approach for analyzing the financial sector's impacts on cybercrime. The author claimed that the changes in financial companies' strategic priorities, with the protection of customer trust and loyalty as the most severe concern, and considerations regarding competitors' market positioning, are essential factors in determining the cost of cybercrime[7].

According to Saiful, Akter, and Zahed (2017), financial fraud activity predicate offenses can be reduced primarily by observing the involvement of local criminals and their involvement with foreign networks and by implementing stringent anti-corruption measures such as digitalization and automated processes in the National Board of Revenue, adoption of a strict criminal identification policy, and assistance from foreign experts. In addition, they gave information regarding Bangladesh's position in terms of financial fraud according to the Basel AML Index Score[20].

Joveda, Khan, and Pathak (2019), emphasized the importance of developing a conceptual framework for preventing cyber-crime in the financial industry of Bangladesh. It is essential to acknowledge how the security approaches in a financial framework potentially influence such illegal activities, consequently leading to a significant loss of economic development. The financial scam has become a threat to Bangladesh's economy[33]. Hence this study aims to develop a cybersecurity framework for identifying it. The author claims that cyber-crime in the banking industry may be reduced by using updated technology and assigning skilled human resources.

In 2018, Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton showed a variety of data theft cyber-attacks on financial organizations, emphasizing the importance of understanding the propagation trends of harm so that we can predict the likely harm will be in future attacks and put measures in place to mitigate it. The author advocated a kill chain lense as a defensive approach around the kill chain, investing in incident defenses and incident response related to reducing the organization's losses[24].

Inaki Aldasoro, Jon Frost, Leonardo Gambacorta, and David Whyte proposed two solutions to cyber risk in the financial sector during covid-19 as a growing work from home situation, the business institution has to adopt this situation as a long-term case scenario, and they have to concern about using public cloud and software as the number of a user is increasing[46]. There have severe types of cyber threats. Secondly, he suggests some ware game and simulation of cyber-attack so that these drills can aid in identifying weaknesses as well as improving readiness and communication.

In another study, the authors provided a wide range of procedures in this study[41]. First, they demonstrate the Risk Detection Process, in which they offer a technique for assessing financial risk by selecting clustering algorithms based on a variety of traditional decision-making procedures. They then discuss the Authentication and Access Control Mechanism process, including cryptography-based methods and ontology techniques. The writers next focus on the protection of the data usages process. This approach extensively uses temporal, location, and authentications based on proximity and privacy issues. Finally, the authors show the secure data processing and storage framework, risk reduction and prevention, fraud detection, and accounting fraud detection.

Jennifer Callen-Naviglia and Jason James developed another thesis (Callen-Naviglia, 2018)] on the significance of Fintech, Regtech, and cybersecurity, where each component is well defined with its immediate and long-term advantages[25]. Furthermore, they linked specific examples, such as the 9/11 assault, to the significance of cyber-

security. They recommended the enhancement of cybersecurity as a tool for safety and FinTech goods and services to be presented as a solution.

A. Sarvana and S. Satyaha Barma's article emphasized the significance of cyber security and the numerous threats that exist in today's digital world[36]. In essence, their study discusses fifth-generation cybersecurity architecture. They also discussed the real-world cyber security problem and the advantages and drawbacks which is the deployment of fifth-generation security architecture. Furthermore, they highlight several sectors of Cyber Security and briefly present a few forms of attacks. Surprisingly, they displayed the percentage of assaults that exploited a new vulnerability.

The research work [(Nikhita Reddy Gade, 2014)] outlines the Challenges and Emerging Trends in New Technologies. Nikhita Reddy Gade and Ugander G J Reddy created an outstanding introduction that included information on cybersecurity and crimes[8]. Their study focuses on what security methods may be used during a cyberattack and how these assaults might be carried out in the network.

Summarizing the given solutions, all the researchers focused more on precaution than prevention, which goes with the hypothesis of this study too. Nevertheless, newer technologies should be adopted to keep the infrastructure safe and up to date. Hence, this study would show a framework where a possible precaution and prevention will not drop; instead, a comprehensive one summarizing every possible solution will respond to the threats and attacks.

Chapter 3

Research Activities

The research's primary objective is to establish a framework that will make the fintech business safer for individuals and enterprises. The initial step is to gather as many fraud cases as possible to make it successful. As the study focuses on attacks targeting both end-users and organizations, classifying victims into two is important after gathering the case studies.

Before portraying the main types of attacks, one of the most critical findings is how hackers, scammers, or attackers open the gate of reconnaissance, which is the very first step of all sorts of hacking[6].

A study on social engineering says that almost 71% of employees fail just because of social engineering. In terms of end-users, nearly every single scamming case succeeded just because of the silly mistakes of the end-users, which leads to leaking their essential personal and financial information[59]. Hence, finding common steps and traps hackers use to get the credential is one of the primary objectives of the work plan.

Finding effective prevention of other attacks targeting the fintech industry is one biggest goal after separating cases from social engineering. To find the optimal prevention, it is essential to compare points from a global perspective.

Finally, the study aims to create a framework for users and organizations. It will show a pathway using newer technologies like blockchain to prevent the most common attacks and keep funds safe and secure from scammers and hackers[32]. However, the attackers get the colossal passion to target in a new way every day; the framework would not ensure absolute safety from being scammed. Instead, it will always look for more contemporary case studies using the latest hacking methodology and find better preventions.

The following figure shows the sequential activities of the study -

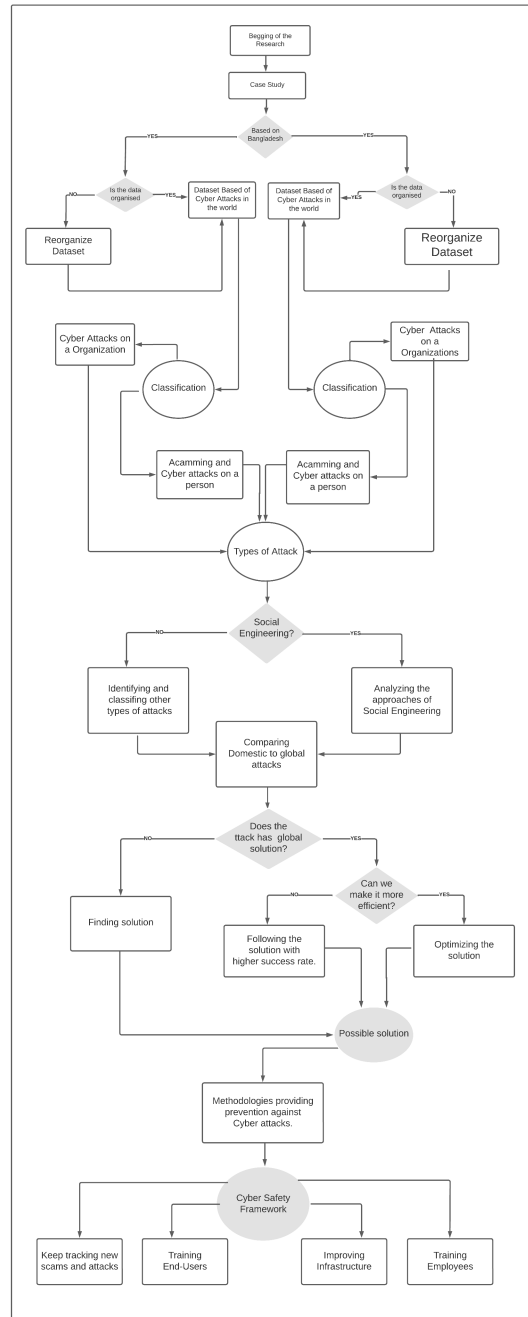


Figure 3.1: Research Activities

3.1 Methodology

The following diagram shows how the research team works with all the datasets for the study. It offers a detailed overview of the method used to find the best outcome. All the portions of the flowchart are described in detail in the next section.

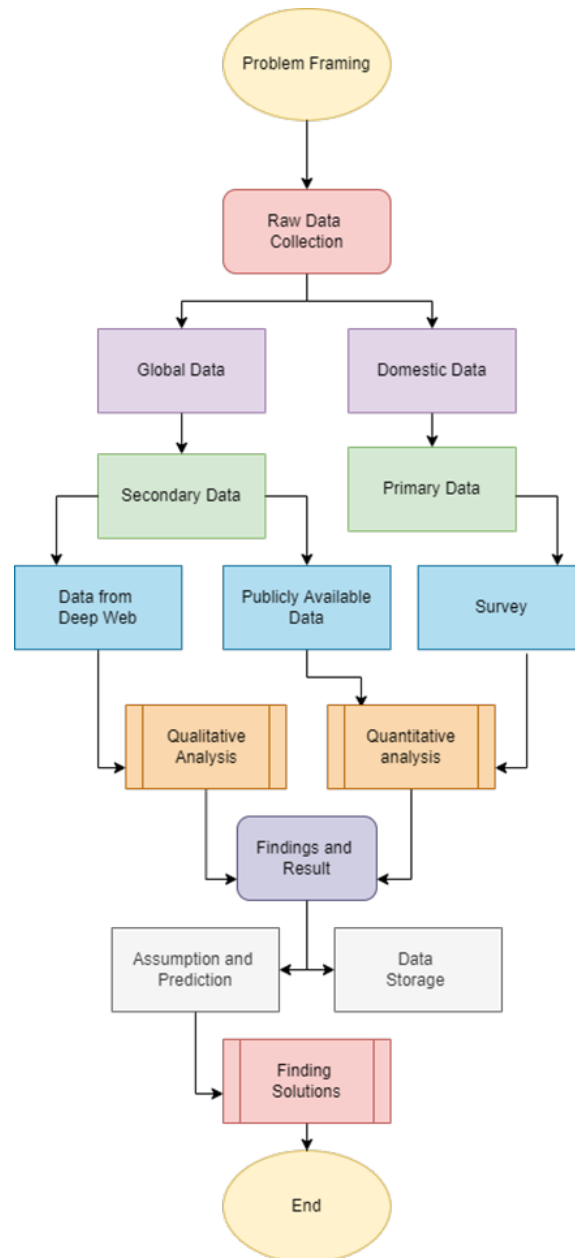


Figure 3.2: Methodology

Chapter 4

Data Description

4.1 Problem Framing

This research expresses all the attacks on financial organizations, including mobile and regular banking. Hence, every case where end-users or organizations related to financial activities attacked attackers succeed or not is included in the dataset to create more considerable problem framing.

4.2 Data Collection

For this research, we performed multiple steps to gather information and prepare the datasets.

4.2.1 Collecting Raw Data

Raw data were collected for only the domestic context very sensitively to get an idea of the accurate picture of the problem. The research team collected raw data using Google Forms and a survey; however, the data was confidential, so the users and organizations wanted to provide them anonymously.

4.2.2 Global Data

The study uses openly accessible different datasets developed by proficient research teams. A global dataset was used by training a machine learning model which shows the authenticity and fraud over money transactions. The model is described. Then, the global dataset was analyzed, and it was found to specify the different kinds of cyber attacking methods used in financial organizations worldwide.

4.2.3 Domestic Data

In the context of Bangladesh, there are not enough publicly accessible datasets on financial services, especially in the rising mobile financial service domain. Financial

datasets are essential to many researchers, particularly in fraud detection research. The intrinsically confidential aspect of financial transactions leads to the lack of publicly available statistical data. So, a few financial scam information was collected about Bangladesh by creating a google form and taking data from various authentic internet sources.

4.2.4 Primary Data

As there was no structured data in the relative problem, the research depends on primary data in terms of domestic cases. After justifying the cases, every possible data was collected. Because of broader use cases of Mobile banking in Bangladesh, enormous raw data was found primarily.

4.2.5 Data from Survey

The research team reached many victims who got scammed in the last few years. This study collected raw data without manipulating and cross-checking the cases. Some interviews took place both in-person and virtually to get the best possible output.

4.2.6 Secondary Data

Financial services came under the umbrella of technology worldwide. Hence, many victims got scammed, and attackers usually sell victims' data on the dark web. The research relies on different organizations that collect and post them on public internet networks. The research depends on the different publicly available datasets as the secondary data for the study.

4.3 Datasets

4.3.1 PaySim Synthetic Financial Dataset

The first dataset analyzed in this study is a synthetic financial dataset developed by the PaySim simulator. PaySim generates a synthetic dataset using processed data from the private dataset that replicates the effective development of transactions and injects malicious activity to study the reliability of fraud detection methodologies.

4.3.2 BankSim Dataset

The second dataset used in the study was Banksim Dataset. It is a framework that refers to an agent-based framework for the banking sector.

4.3.3 Socradar Dataset from Deep Web

The third and most crucial dataset used in the study was collected from "Socradar" a cloud-based autonomous service recognized by a million professionals in the cybersecurity world. Socradar collects financial data breaches from the deep web and

posts them on its official website. The research team scrapped all the financial data breaches from January 2020 to January 2022. Then the team conducted “Qualitative Data Analysis” and came up with multiple crucial findings and results, which are all described briefly in the following sections.

4.3.4 Other Datasets

The research team uses multiple datasets excluding the mentioned ones to get a better understanding of which were mentioned in the relative sections.

4.4 Data Processing

Data were processed to find a meaningful outcome from the raw data collected in the previous step, keeping all the conventional steps ahead.

4.4.1 Editing of Data

The research team kept it as accurate as possible for the initial stage. Raw data were double-checked for repetition. The quality was also assured in the step. Central Editing and field editing was needed for some cases. Lastly, for the tabulation, raw data was edited once.

4.4.2 Coding of Data

Different symbols and numerals were given for the respective fields to process the data in an organized manner, which assures the coding of data.

4.4.3 Classification of Data

Data were classified into different sections for the next step.

4.4.4 Tabulation of Data

Tabulation was implemented conventionally to summarize all the raw data.

4.4.5 Data Diagrams

Finally, to get the idea more visually, data is presented in many data diagrams, including Graphs and Charts.

4.5 ML Model

The research uses the ML model for in-depth data analysis for domestic and international financial fraud cases. The team used the XGBoost algorithm to find the data described in the following section.

4.5.1 Extreme Gradient-Boosted (XGBoost) Algorithm

The research team uses the XGBoost algorithm in the PaySim Synthetic dataset to classify fraud and authentic transaction detection.

The research team selected XGBoost over other options to find the best output. The algorithm uses additional previous probability to find out the similarity score.

$$\text{Similarity Score} = \frac{(\sum_{i=1}^n \text{Residual})^2}{\sum_{i=1}^n [\text{Previous Probability}_i * (1 - \text{Previous Probability}_i)] + \lambda}$$

Equation 4.1 : Similarity Score of XGBoost; Source: towardsdatascience.com

Here, Residual refers to “actual (observed) value — predicted value”

After finding the similarity score, the algorithm calculates the gain value.

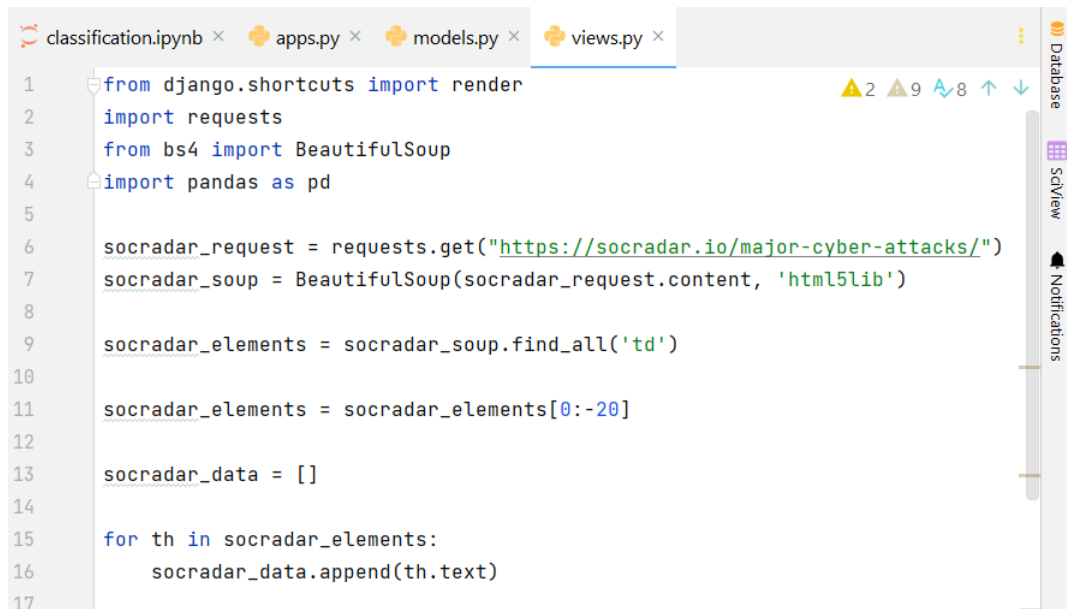
$$\text{Gain} = \text{Left leaf}_{\text{similarity}} + \text{Right leaf}_{\text{similarity}} - \text{Root}_{\text{similarity}}$$

Figure 4.1: Output of XGBoost; Source: towardsdatascience.com

4.6 Web Scraping using BeautifulSoup

As most of the stolen data are sold on the deep web. So, the research team collected secondary data from a Security Threat Intelligence Services provider, Socradar. The team found a large dataset available on the website.

To scrap the data from the website, the research team used “BeautifulSoup,” a scrapping library along with other libraries like pandas, requests, and render.



```
classification.ipynb × apps.py × models.py × views.py ×
1 from django.shortcuts import render
2 import requests
3 from bs4 import BeautifulSoup
4 import pandas as pd
5
6 socradar_request = requests.get("https://socradar.io/major-cyber-attacks/")
7 socradar_soup = BeautifulSoup(socradar_request.content, 'html5lib')
8
9 socradar_elements = socradar_soup.find_all('td')
10
11 socradar_elements = socradar_elements[0:-20]
12
13 socradar_data = []
14
15 for th in socradar_elements:
16     socradar_data.append(th.text)
17
```

Figure 4.2: Web scrapping using BeautifulSoup

4.7 In-depth Data Analysis

The research refers to in-depth data analysis for both domestic and international cases in terms of financial fraud cases.

4.7.1 Inferential Analysis

Inferential analysis was used mainly for mobile banking scams in domestic cases.

4.7.2 Predictive Analysis

Predictive analysis was used compared to international fraud cases. From the perspective of Bangladesh, these attacks may occur shortly.

4.7.3 Qualitative Analysis

As a broad number of data was collective and non-numerical. Hence, the qualitative analysis took place significantly. Information collected from social media and newspapers went through content analysis. Both "Narrative" and "Discourse" analysis was successfully done for the non-numerical information. Lastly, "Grounded Theory" was implemented to find a distinct point of the analysis.

4.7.4 Hypothetical Analysis

This kind of analysis was used to clarify some predictions.

4.7.5 Interpreting the Results

After carefully going through the previous steps, the research shows a powerful, alarming message regarding domestic and international perspectives. The findings from the data were visualized using different tools and standard machine learning models to get a better overview and the prediction.

4.8 Data Storage

For the future study, data was stored in a well-mannered along with all the charts, graphs, and diagrams.

Chapter 5

Analysis and Findings

5.1 Based on PaySim Synthetic Financial Dataset

PaySim synthetic financial datasets primarily consist of simulated MFS transactions based on a model of accurate money transfer taken from one month of financial history from a widespread African nation's mobile payment service. The first few records are added by a multinational corporation that operates an MFS nowadays available in over 14 different countries worldwide. For this study, the research team scaled down 1/4 of the original dataset, and this dataset contains the transaction types - Cash-In, Cash-Out, Payment, Send Money, and other categorized columns. Hence, in the following table, an instance of the description of a dataset.

step	type	amount	nameOrig	oldbalanceOrig	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud	
0	1	PAYMENT	9839.64	C1231006815	170136.0	160296.36	M1979787155	0.0	0.0	0	0
1	1	PAYMENT	1864.28	C1666544295	21249.0	19384.72	M2044282225	0.0	0.0	0	0
2	1	TRANSFER	181.00	C1305486145	181.0	0.00	C553264065	0.0	0.0	1	0
3	1	CASH_OUT	181.00	C840083671	181.0	0.00	C38997010	21182.0	0.0	1	0
4	1	PAYMENT	11668.14	C2048537720	41554.0	29885.86	M1230701703	0.0	0.0	0	0

Figure 5.1: An instance of PaySim Dataset

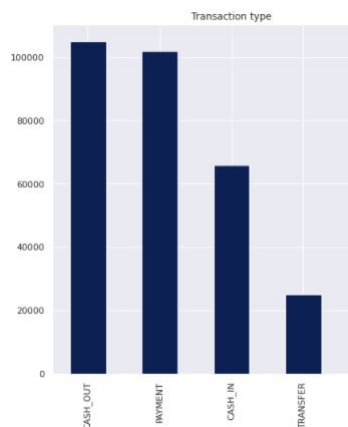


Figure 5.2: Different Types of Transactions

5.2 In-depth Analysis

The study team analyzed this dataset and discovered that fraud happens in two of the five different types of transactions.

The first option, known as Transfer, involves sending money to a consumer, while the second, known as Cash-Out, involves sending money to a retailer while the customer is paid in cash. Surprisingly, the number of fraudulent transfers is shockingly close to matching the number of fraudulent cash-out operations. Within this two-step operation, the fraudulent account would function as the recipient in a TRANSFER and the source in a CASH OUT transaction. On the other hand, the data for Transfer and Cash-out accounts are displayed in the figure among the fraudulent transactions. Whenever there is an attempt to "TRANSFER" a "amount" that is more than 200,000, the data gets tagged as "isFlaggedFraud." The isFlaggedFraud flag may not be set for genuine transactions even if the criteria are met. For this condition, the research team chose to disregard newBalanceOrig since it is only modified after the transaction, whereas isFlaggedFraud is set before. When isFlaggedFraud is set, there are no duplicate customer names displayed; on the other hand, when it is not set, the same customer names are displayed. The following figure demonstrates

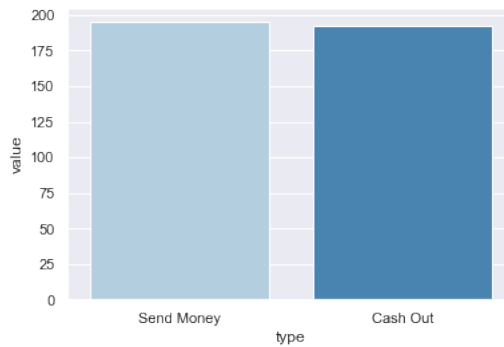


Figure 5.3: Fraud Distributions

how the fraudulent and authentic transactions have different characteristics if the dispersion is analyzed over time. It is observable that fraudulent transactions are more homogenously scattered across time than authentic transactions.

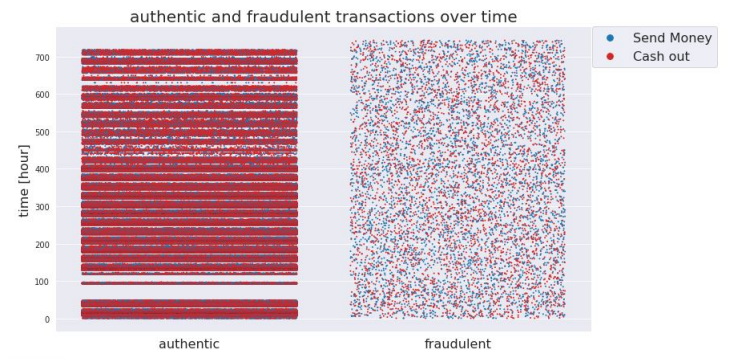


Figure 5.4: Transactions Over Time

Several transactions in the dataset result in zero balances being left in the account. To ascribe the account balance, we do not utilize a statistic or a distribution followed

by a subsequent adjustment for the amount that was transacted. This occurs before the transaction is made. It is because destination accounts with negative balances are an essential indicator of fraud. Additionally, the evidence demonstrates many. The transactions in which the originating account had a zero balance both before and after a transfer of a non-zero-sum are referred to as zero-balance transactions. These kinds of transactions have an extremely low fraud rate (0.3%), far lower than real transactions (47 percent).

The data contains extensive information so that an ML algorithm can generate influential assumptions and visually see the differences between fraudulent and authentic transactions.

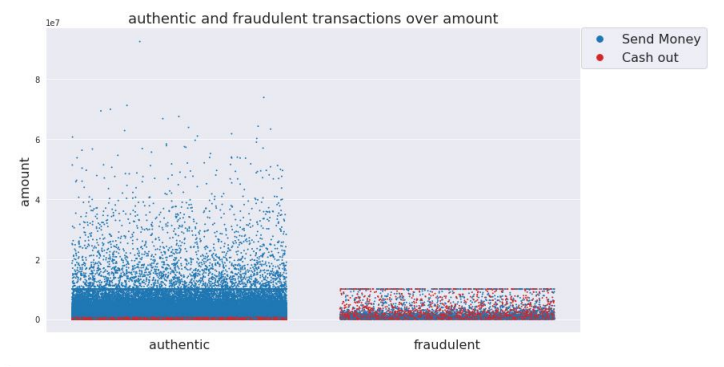


Figure 5.5: Transactions Over Amount

5.3 Based on Deep Web Dataset

Data collected from the deep web via Socradar[65] shows significant attacks where some are very common and some are new in the industry. The research team initially scrapped the report for 2020 cyberattacks leaked in Darkweb using the python “Beautifulsoup” library.

5.3.1 Attack Types

The study shows the most common seventy (70) attacks that occurred worldwide since 2020. The attacks are also classified in some broader sections. The attacks were described in the publicly available database, found on the deep web posted by the hackers and attackers.

Spear Phishing	Specified Attack on a specific person.
Watering the Hole Attack	Divert the group of users to the malicious site.
SPIM	Instant message spamming.
Vishing	It is a type of phishing using phone numbers, voice, and text messages.

Table 5.1: The most common attack types that occurred all over the world

Smishing	Trying to obtain logins or other personal data through a malicious message.
Reconnaissance	Refers to collecting all possible information about the target.
Credential Harvesting/ Account Harvesting	The way of collecting users' personal information
Pharming	The way of traffic manipulation and stolen information by DNS poisoning.
Dumpster Diving	Removed data collection from the device.
Shoulder Surfing	Stealing password using MFA or OTP.
Tailgating	A type of social engineering helps access a protected area.
Typo-squatting	Type of social engineering targets the incorrect URL typed by users.
Malware	It has designed software to destroy a computer, server, or network.
Trojans	The way of installing malware.
Remote access Attack	It remotely accessed Trojans.
Virus	used to destroy computer systems.
Worms	Type of malware replicates itself.
Crypto Malware	Refers to cryptojacking activities that occur in computers.
Bots Agent Software	Take instructions and follow them accordingly.
PUP	Sort of software which has been installed without the user's permission.
Fileless virus	A PowerShell script that does not have any file system and leaves no footprint.
Armoured	A reverse engineering technique.
Keylogger	Keep records of what has been typed on the keyboard.
Logic Bombs	Refer to doing something when a logical condition is met.
Rootkit	Type of malware, create a malicious software package designed to allow unauthorized access to a computer.
Brute Force	Make every possible combination of encryption keys.
Dictionary	This is a list of expected search passwords.
Online vs. Offline PW Attacks	Compares hashes (for offline, around five days)
Rainbow Table	A table for precomputed hashes function.
Supply Chain Attacks	It targets the third-party vendors of the supply chain.
Cloud-Based Attacks	It keeps eyes on cloud architecture
Collision	In cryptography, a collision attack seeks to discover two inputs that produce the same hash

Table 5.2: The most common attack types that occurred all over the world

Downgrade	A network channel is forced to convert to a less secure data transmission standard by an attacker.
Injections	Find the type of database and input it. An interpreter processes this input as part of a command or query.
Cross-Site Scripting	Malicious scripts or codes are inserted inside websites that are secure and reliable.
Prevention	A strike was conducted to dissuade foreign troops from launching an attack.
Poorly Written Apps	Fraudsters get unlawful access to local places.
Overflow Attack	Attack using buffer overflow bugs.
Impersonation Attack	Make a fictitious email account that appears identical to the real one.
Error Handling Attack	Divulge information about technology that should not be disclosed.
SSL stripping	Degrade a site interaction from HTTPS to HTTP, which is less protected.
API modification	Using exploit, the data is sent into an API to get access to the website's content and manipulate or destroy it.
Driver manipulation	To interface with equipment tools or relevant factors, you will need to employ adapters.
Wireless Attacks	Harmful behavior directed at high bandwidth data or cellular routers
Evil twin	Fooling visitors into enrolling in a phony Wi-Fi gateway that behaves like a real network
Shadow IT	Without the consent of the IT sector, the use of any prohibited or unauthorized computer systems.
Bluesnarfing	To gain data access via Bluetooth enabled wireless connections.
Bluejacking	Delivers unwanted contents to wireless connections.
Attacks in IoT	The conduits through which IoT objects communicate with others.
DHCP configuration	The attacker sends falsified DHCP queries to DHCP servers with the goal of disturbing all usable Ip's that the DHCP server might assign
ARK Spoofing	Enables hackers to eavesdrop on network traffic.
Unauthorized L3 Router	Network flaws, network software discrepancies, and insecure verification.
Redirecting by using DNS Spoofing	A security breach which deceives your pc into considering it is visiting the accurate website when it is not.

Table 5.3: The most common attack types that occurred all over the world

Man in the Middle	Type of engaged mass surveillance strike where the striker wiretaps and carefully alters conveyed evidence in order to impersonate several of the organizations.
Address Resolution Protocol	A LAN strike where a bad attacker transmits forged Packet data.
ARP poisoning	Utilizing ARP flaws to deceive its MAC-to-IP lookup tables of other connected devices.
Mac Flooding	Aimed at compromising the security of the switch ports.
MAC Cloning	Includes altering a related MAC address (network card).
IQ Ethernet Trunking	A means of targeting connected assets using a digital LAN
DoS Attack	An opportunity to bring a system or network to a halt, rendering it unreachable to its target purposes.
DDoS Attack	Render an online site, web service, or host system inaccessible to its targeted Web users.
STP (Spanning Tree Protocol)	Can change logical topology, an attacker is impersonating the topology's root bridge.
Domain Hijacking	A third party steals a company's URL.
DNS poisoning	DNS servers are being used to reroute data traffic to a fake site that looks like the one targeted.
URL redirection	Redirect the platform's visitors to an untrustworthy affiliate location
DNS Tunnelling	DNS requests and replies. It encrypts data towards other processes or networks.
Domain Reputation	Is the state of your trademarked site's wellness.
Botnet	A massive assault conducted by infected machines that are centrally directed.
Sim Card Spoofing	Transferring mobile number into another device
log4j	Code execution remotely, based on Java

Table 5.4: The most common attack types that occurred all over the world

These cyberattacks of various forms are occurring in several areas throughout the world. In most situations, the primary target of attackers is a financial institution. After processing the raw data and keeping only financial cases from Socradar, it shows that from 2020 to 2022, Phishing was a primarily used kind of attack that happened through 35% of total episodes, and a total of 324 attacks occurred using it, which is the most used type of attack throughout this time. The second most used type of attack is Malware, which is 28% of the total number of incidents, almost 258 times. Another mainly used time of attack type is gradually Ransomware, Partnership Searching, and tools, and those are the 5%, 8%, and 5% of total attacks. Besides, there are more attacks: SQL Injection, DDoS, Trojan, RDP, Bot Carding service Bypass, and the Rat type of attacks happening nowadays.

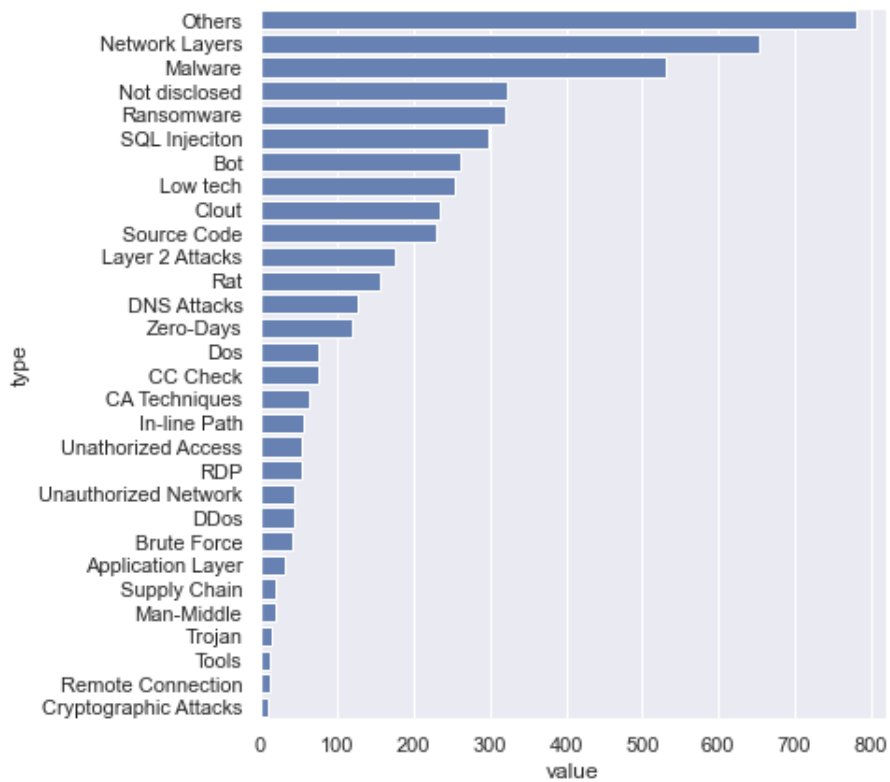


Figure 5.6: Common Cyberattacks

Chapter 6

Cyberattacks in Broader Categories

Different assaults utilize distinct procedures. The research summed up them into some broader categories. According to the previous dataset, the most common sort of attack from 2020 to 2022 was the "Cyber Attack Method," with over 13 distinct variants of this technique being utilized. The second most common assault was "Application Attack," utilized in 11 different ways.

On the other hand, "Social Engineering" and "Layer 2" are the most popular assaults, and both are deployed in eight different ways. Furthermore, utilizing "Network layer Attack," "In-line/On-path Attack," and "DNS type," six types of attacks progressively occurred. Other regularly utilized assaults include "Password Attack" and "Low Tech Attack," both used for six distinct types of attacks. Many forms of attacks are occurring in the IoT environment, including "Supply Chain Security," "Cryptographic attacks," and "Zero Day Attack."

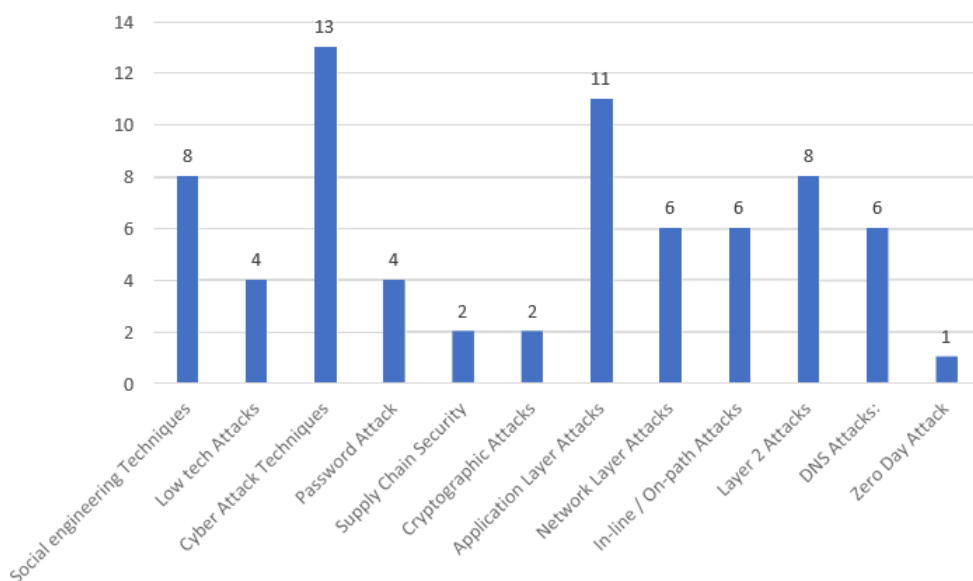


Figure 6.1: Cyberattacks in Broader Categories

6.1 In terms of Bangladesh

After processing the secondary data collected from different publicly available sources, it is clear that most of the attack types in Bangladesh are Ransomware, which is very alarming for our national security concern. Moreover, second most known types happened because of Social Engineering (29%). Then Malware is having a percentage of 16%, and 10% of total cases are still unknown.

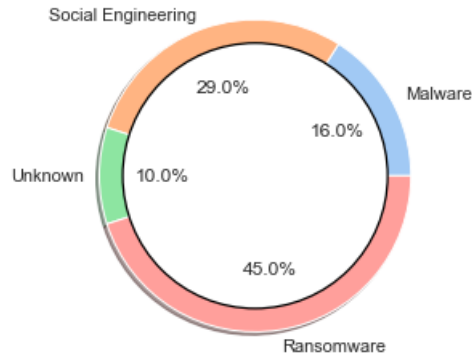


Figure 6.2: Cyber-attacks in Bangladesh

6.2 Affected Countries

The following graph shows that most cyberattacks occurred in the United States of America. Besides, Russia, China, the UK, Spain, and Germany are also highly affected, including France, Mexico, Italy, India, and Australia, and day by its being alarming for all over the world. The bulk of robberies targets the internet and its users, with most victims coming from developed and developing nations.

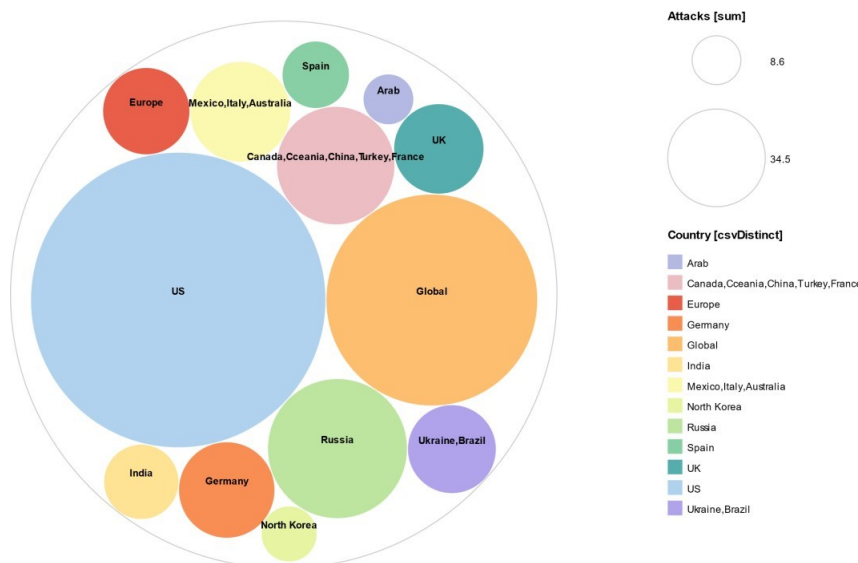


Figure 6.3: Countries affected by massive cyberattacks more than 10 times

6.3 State-Backed Hackers

The research predicted significant involvement of “State-BackedHackers’ Group” targeting their rivals in this field. The research team found a dataset from the “Center for Strategic International Studies”[62].

The dataset shows how different countries are attacking their rivals directly and backing up hackers. The research Team collected raw data by web scrapping, and after using machine learning models, the research team found similarities that showed the prediction was correct. The following figure shows the output of the data analysis.

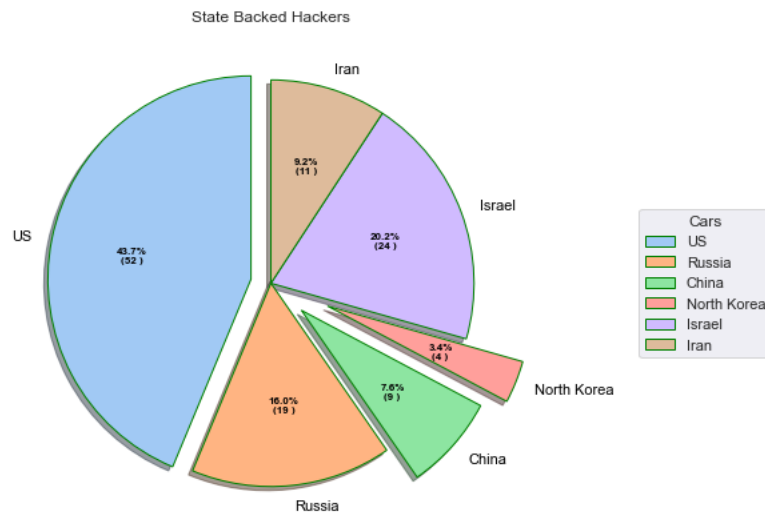


Figure 6.4: State Backed Hackers

The figure shows that most of the attacks were funded by the United States, about 43.7 percent. Moreover, Russia, Iran, North Korea, China, and Israel supported 16%, 9.2%, 3.4%, 7.4%, and 20.2% of attacks.

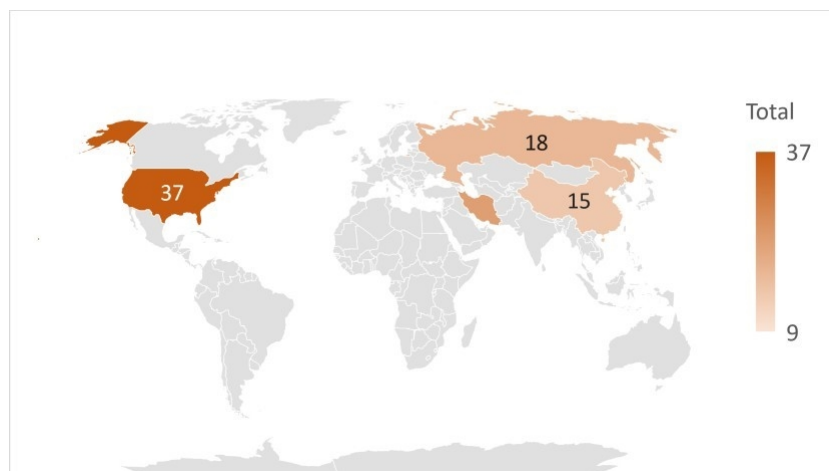


Figure 6.5: Targeted Countries

The figure shows that most attacks were targeted at the US, where Russia and China are in the second and third positions.

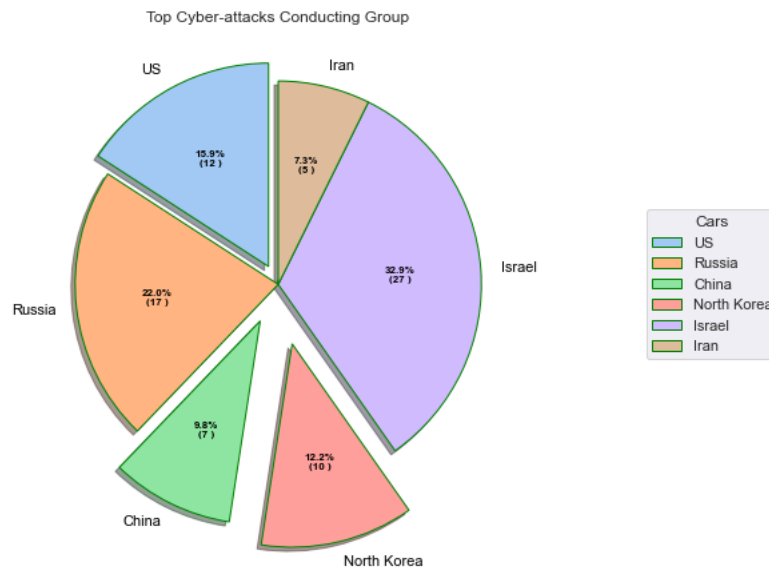


Figure 6.6: Nationality of Cyberattacks Conducting Groups

The pie chart shows that Israeli attackers carry out most cyber-attacks, which account for about 32.9%. In addition, the USA, Russia, China, North Korea and Iran, are 15.9%, 22%, 9.8%, 12.2%, 7.3%, respectively.

6.4 Attacks on Different Financial Activities

Every day, the financial institution must deal with millions of transactions such as cash in, cash out, and balance transfers, and they must rely on online transactions in most situations. As a result, the most sophisticated cybercriminals concentrate their efforts on financial transactions. As a result, thousands of attacks occur every second.

Nowadays, most payments are made online, making it a lucrative opportunity for thieves. According to the graphs, the 354873 assaults happened when someone attempted to pay for anything online.

Furthermore, 373641 attacks occurred when they attempted to withdraw money from a financial institution such as an ATM or mobile bank, 227130 attacks occurred when they attempted to deposit money into their bank account, and 86752 attacks occurred when they attempted to transfer money.

Debit cards have also been targeted by cybercriminals, with 7187 incidents reported. According to statistics, online transactions are exceedingly hazardous and are becoming more so.

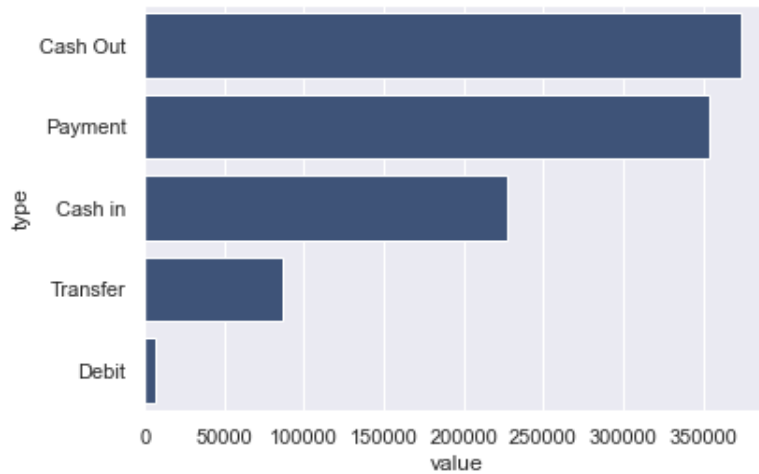


Figure 6.7: Attacks on different financial activities

6.5 In terms of Gender

The gender-based attack percentage and number are shown in the dataset scraped from "socradar.io," which surveyed over one million people. According to the pie chart, from 2020 to 2022, 324565 women, or 53 percent of the victims, were targeted by cybercriminals. On the other side, 44 percent of male users (about 268385) were affected at the time.

The assailants are more likely to target a woman than a guy since women are more easily manipulated. Furthermore, they are unconcerned about their transaction, and attackers can exploit them with their tools.

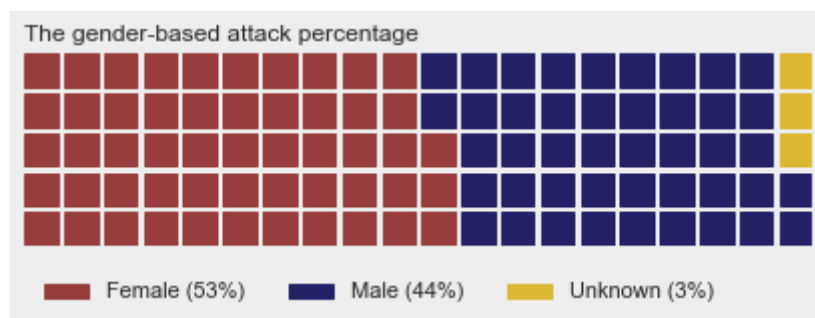


Figure 6.8: Classification in the context of gender

Chapter 7

Cyberattacks in Bangladesh

The financial sector of Bangladesh is vulnerable to cyber-attacks, and several doubts are being raised regarding financial institutions' precautionary action. According to the Bank Management investigation of Bangladesh, 43% of events occurred via ATM cards, 25% via mobile payments, 15% via ACPS and EFTN, 12% via online payments, 3% via source code, and 2% via other means.

Consequently, the significant abuse and cyber-attacks in Bangladeshi banks during the last few ages are spotlighted. In one of the massive cyberattacks in the history of the world, the attackers, whom U.s police confirmed were associated with North Korea, were using malicious requests on the SWIFT payment service to grab US\$951 million from Bangladesh bank's wallet, nearly all of the cash inside that vault.

However, the end-user is typically the most prominent concern regarding cybersecurity, which assailants take advantage of. Maybe that is why phishing has become an effective way of distributing malware.



Figure 7.1: Cyberattacks in Bangladesh

7.1 Attacks on Financial Zones in Bangladesh

The following figure displays the cyber-attacks on various financial zones in Bangladesh. It shows that 46% of MFS users have been affected by cybercriminals, and 19% of Banking organizations, and 35% of ATM users were affected due to these criminal activities in Bangladesh.

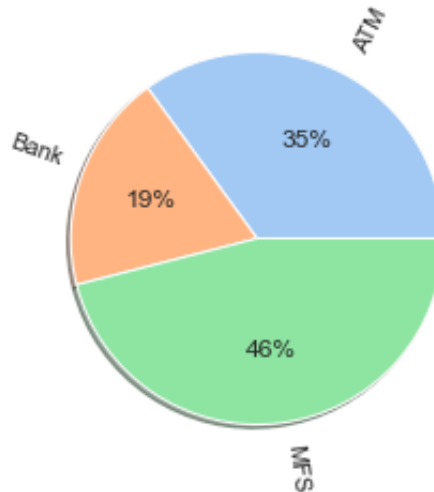


Figure 7.2: Attacks on financial zones in Bangladesh

MFS suppliers, payment processors, and money transfer companies should be watchful for cyber threats and breaches used in electronic transfers.

Also, there was substantial growth in the number of banking firms that malicious hackers attempted to breach. Various cyberespionage clusters compromised the bank framework, e-money mechanisms, virtual currencies, capital allocation investments, and casinos. Their primary objective was to pull back considerable amounts of money. Hackers make decisions based on tried-and-true methods of commercializing internet connectivity to accomplish their cybercrime practices.

ATM strikes seem to be noteworthy in their own right. The first ATM threat actors popped up in 2009, and from then on, such machines have been the focus of computer hackers. The advancement of this form of threat seems to have been constant. ATM malware-as-a-service has emerged in the last year, and then the following process will be complete mechanization of these attacks – a special edition will be easily linked to an ATM, resulting in malware insertion and associated with behavioral or card information gathering. This dramatically reduces the time required for invaders to dedicate to their violent acts.

7.2 Cyberattacks on Different Geographic Areas in Bangladesh

The following pie chart exhibits the result of cyberattacks on different geographic areas in Bangladesh, where the Banking system and MFS both are active. In this

case, it is seen that urban areas suffer more than rural areas. In urban areas, 67% of the user face illegal operations while making a transaction, whereas, in rural areas, 33% face money laundering issues during the transaction. The ratio of the survey is 1:2.

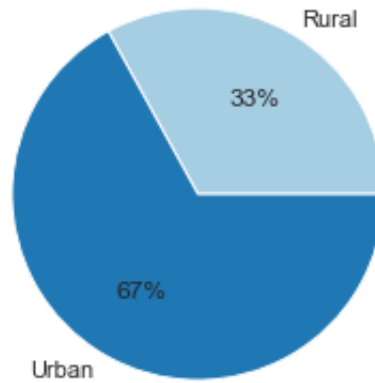


Figure 7.3: Cyberattacks in different geographic areas in Bangladesh

7.3 Cyberattacks on Mobile Banking in Different Geographic Areas in Bangladesh

Previous surveys found that cyberattacks were more prevalent in urban areas than rural areas. Nevertheless, from the above chart, we can see the survey of the cyberattacks on mobile banking in rural and urban areas of Bangladesh from 2019-to 2022. It is visible that most of the attacks took place in rural areas, which amounted to 70%, and 30% of Urban areas were affected by the hackers. The main reason for more attacks in rural areas is not having minimum knowledge about cyberattacks.

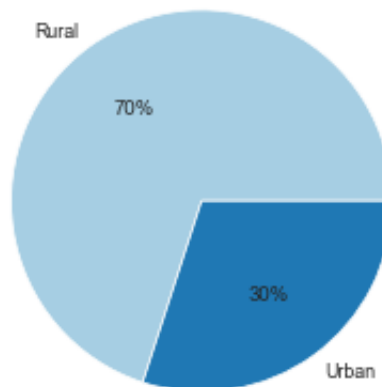


Figure 7.4: Cyberattacks (MFS) in different geographic areas in Bangladesh

7.4 Attacks on Mobile Banking in Bangladesh

The following figure displays the illegal operations on mobile banking or digital payment. The survey was conducted on the mobile banking system of Bangladesh from 2019-to 2022. It shows that in the case of mobile banking, most of the criminal activities have taken place while cashing in. The second-largest money laundering occurred during cash out. Furthermore, the lowest amount of robbery took place while sending money.

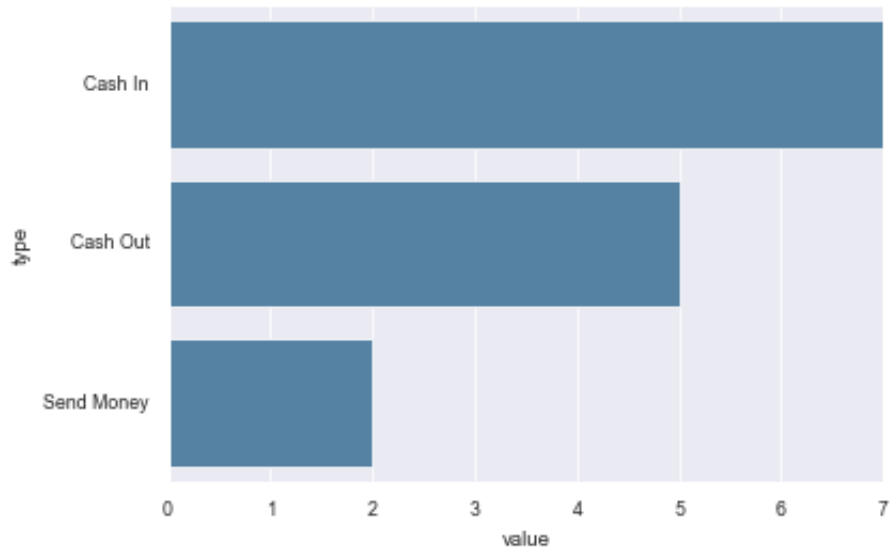


Figure 7.5: Attacks on Mobile Banking in Bangladesh

Chapter 8

Result and Discussion

Different sorts of Cyberattacks are taking place around the world. Phishing was the most familiar form of threat, accounting for 35% of all occurrences. Several threats are DDoS, Trojan, RDP, Bot Carding service Bypass, and Rat malicious behavior. The "Cyber Attack Method" was perhaps the most prevalent sort of violence from 2020 to 2022, with over 13 unique, different versions of this methodology being used. Other frequently used strikes include "Password Attack" and "Low Tech Attack," used for six various types of attacks. In the IoT environment, many kinds of damage are taking place, along with "Supply Chain Security," "Cryptographic Attack," and "Zero Day Attack." The significant proportion of recognized incidents in Bangladesh is still unidentified, which is hugely concerning for our domestic security. Social engineering accounts for 29% of all breaches, while malware records for 16%. Ransomware accounts for 10% of all cases, while Crypto Molecular malware accounts for only 0.1%. According to another study, many incidents focus on online services and their consumers, with most victims emerging from both industrialized and developing economies[34].

According to the survey, most cybercrime is reported in the USA. Russia, China, the UK, Spain, and Germany are also severely impacted. The research group discovered a set of data from the "Center for Strategic International Studies" that demonstrates how various regions are constantly targeting and supporting attackers. The research group gathered raw data by web scraping and then used machine learning models to compare the forecasting accuracy.

According to Babu, K. -E. -K, along with the modern world, the economy of Bangladesh is advancing at a fast pace, which has resulted in a strong relationship with the digitalized economic system[43]. As a result, Bangladesh is also at a high risk of cyberattacks. Many incidents have already occurred on the financial instruction line in banks, corporate offices, and business institutions. Nevertheless, the primary data shows that the victim is the end-users in most cases. When the team analyzed the attacks, it was found that many attacks took place on MFS (Mobile Financial Service), which is about fifty percent of total attacks, including banking and ATM, which is also at high risk for a cyberattack.

The study also shows that most of the attack occurs in the urban area as the user rate is much higher than in the rural area. However, from a mobile banking per-

spective, most of the incident occurs in rural areas, which is about seventy percent of the total attack. According to The Daily Star, the main reason is that the users do not know the proper use of this online system, and they do not have a fair idea of the use of MFS and hacking procedures[11]. So, the attacker's eye is on them, and they wait for a decent chance. The research shows that attackers mainly use social engineering on the end-users to manipulate them in most cases. Besides, they also use Ransomware, a Malware type of attack on the business organization.

Another report in The Daily Star expresses that the matter of concern is that the organization does not know the kind of attack and how it is occurring in most cases[52]. As a result, they cannot guide their customers in systematic ways. The research team also found that, in mobile banking sectors, most of the attacks happen when the user goes for cash in their account rather than cash out and sends money, and it is an alarming scenario for Bangladesh.

E-banking, digital wallets, or internet money transfers are examples of digital financial services (DFS) that can be retrieved anywhere. There are several obstacles to mobile financial services, such as minimizing financial and technical hazards, ensuring suppliers' potential to supply adequate services to consumers, and thoroughly securing satisfaction levels. The Internet of Things (IoT), blockchain technology (BCT), augmented reality (AR), open APIs, online games (VR), deep learning, advanced analytics, Robo advice, and cloud technology, among other stuff, are crucial accounting. These services have already been comparatively validated in Bangladesh by mobile financial services (MFS) providers, including Rocket, BKash, and Nagad.

MFS in Bangladesh faces a variety of similar obstacles. Plausible cyberthreats, self-concept, concealment, the immediate massive price for entry, secure transactions, self-assurance, lack of appropriate mindset toward a unique product, reduction in money transactions, etc. MFS integration with the latest tech such as blockchain technology, virtual reality, machine learning, and the web helps the MFS sector reach the next level. MFS organizations firmly safeguard their clients' details, have formed risk-free IT connectivity and cyber warfare, and thus interact between them on a regular schedule.

A study shows that financial firms designate an operative to carry out their operations in terms of regular banking. Still, representatives are not very well qualified and experienced as they should be, which may open the door for the subsequent cyberattacks on that company[31].

Hence after analyzing all the studies, it is clear that no matter whether it is an organization or a person, most cyber-attacks can be tackled before they occur by having ground-level knowledge of common attacks - especially phishing and social engineering.

Chapter 9

Solutions

9.1 Existing Solutions

Ambore et al., 2017 show about \$2.1 trillion in data breaches related to financial activities. The researchers also express the three major attacks on SWIFT interbank, including Vietnam, Ecuador, and Bangladesh[14].

The Researchers provide a model to secure the system. In the proposed model, there were five different sub-sectors which are -

- State of Art
- Requirement
- Framework
- Validation
- Exploitation

They also suggested treating financial settlement companies separately and implementing software with a forensic analysis feature. The study provides a solid framework that may lead to a better outcome. Nevertheless, there is a lack of details in theory. However, the framework is not tested in real-life yet.

According to joint research by Bangladesh Bank and Dhaka University in 2017, the central bank may arrange a mandatory introductory (one month) and human psychological (one week) training for the merchants and agents of MFS. The study also suggests having a unique dress code for the merchants[15].

The research also focuses on female participation in both agents and end-users. It emphasizes creating a dedicated team only for the female participants. The study comes up with some crucial decisions like the lack of participation of female users. However, there is not enough discussion of technical issues which can be done to create a secure financial system.

The study by Jiang et al., 2021 shows some innovative ways to tackle the threat of cybercrimes in the Fintech world. The model mainly focuses on scalability, which

is suggested to be ensured by implementing a qualified FinTech Data server and Send-and-Subscribe framework[54]. The research team introduces a new protocol and examines the framework in real-world Taiwan Stock Data. The result of the test run was affirmative.

In the framework, a client would send a retrieval request to the Task-Dispatching interface, which will reply with an auto-generated message queue topic. The message will be used to deliver acquired data, and the client subscribes to that topic message in the queue server. The data will be encoded automatically through the message queue. They suggest using a message queue (MQ) repository pattern to handle multiple client requests.

The research team also shows three different algorithms sequentially –

- Kernel Design for Task Dispatching APIs
- Data Retrieval-based Topic Control Algorithm
- Task Routing Algorithm

The given framework has a great potential to succeed in protecting financial services. However, the lack of instructions for the end-users makes it not complete. In addition, more secure phenomena – Blockchain and cryptography can be used to mitigate the threats.

In another research, Abad-Segura et al., 2021 highly suggest implementing blockchain technology in financial and non-financial organizations, especially in the accounting department[44]. They show that many pieces of research were published focusing on that field and only accept the ideas of those who have immense influence. However, the research team does not provide any hands-on instruction to implement the newer Blockchain technology in any field, including FinTech.

The research of Imerman Fabozzi, 2020 initially provides an in-depth idea of financial verticals. The study marked some cutting-edge technologies as the "Emerging technologies for Financial Services[39]. Surprisingly, the authors included Virtual Reality and Augmented Reality in that bucket. The authors showed a triangle for FinTech, which comprises people, Technology, and Organizations. The research team pointed out that industrial revolution 4.0 refers to technology. Even though the study covers a lot, however, at some point, there was no elaboration of the triangle, especially "Technology."

Gai et al., 2016 proposed a model named "Anti-Counterfeit Deterministic Prediction Model (ADPM)," which uses the Monte Carlo Model-Based Prediction Analysis Algorithm (M-PAA) to evaluate the authenticity of cloud platforms[9]. The model has great potential if it can be implemented more precisely.

According to Shaikh et al., 2017 a new payment system can be integrated with the help of the current NFC-based mobile network system. The research refers to the new schema which does not support the NFC payments[22]. The study shows a pathway to secure a financial system using a cellular Mobile Network. However,

the research does not show any data on why non-NFC payment is inefficient. A more detailed study is required to evaluate the proposed Mobile Banking Payment System (MBPS).

Another study by Coetzee, 2018 shows that rationalizing internal IT systems can be adopted for different financial activities. The researchers show that African NED-bank Group Ltd and Barclays Group Ltd. Adopted the proposed architecture and got a positive result[26].

The study of Crisanto Prenio, 2017 shows a conceptual framework[17], TAM, which has two belief variables -

- Perceived Usefulness
- PEU determination to determine the user intention for any digital product and service.

The research of Astya et al., n.d, summarizes some of the best proposed solutions to tackle the cyber attacks in the industry. Osiris Framework pointed out a very modern and effective way to find the integer bugs in the intelligent Ethereum blockchain contracts with precision. Torres et al. designed it[30].

The study also shows a better approach to overcoming drawbacks, such as the single point failure of a typical PKI system in Blockchain. The main idea is to keep the Certificate Authority (CA) as a form of a non-signed certificate. The encoded hash data is proposed to be stored and controlled by individual financial organizations. This is one of the best possible solutions to secure the application-level financial organization among all the existing solutions. However, the framework should describe solutions to tackle attacks on the end-user level, which is the entry point of most cyberattacks in the current situation.

In their paper, G. Singh et al., 2021 suggest establishing a regulatory sandbox or RS for real-time testing of Fintech products[63]. Additionally, the study makes obtaining license and KYC (Know Your Customer) procedures must create more secure financial applications.

According to Aaron et al., 2017, the "Bank of Canada" study proposes the same KNY procedures and initially obtains a license[13]. The study also suggests adopting Distributed Ledger Technology in-network solution in a fintech organization. Interestingly, the Bank of Canada study says to always keep an eye on the rival organizations and states.

On the other hand, Park Jin, 2015 proposes a new method to secure fintech. The study solely focuses on how to secure the system from the end-user side[10]. Hence, they propose that instead of using OTP, Security Card, PKI, and HSM, new ways such as User Memory and Certificate can be adopted. They also suggest using one channel instead of Situationally two channels. Though the idea is new in the genre, it is not tested yet. Hence, more study and implementation are required to validate the method.

According to another study by the Institute of Electrical and Electronics Engineers, n.d. to create a secure financial system, Consortium Blockchain should be adopted[29]. The main idea of the blockchain system is not to give access grants to everyone. Instead, it is given according to the determination of a group of nodes. Then the study refers to adopting similar ideas, which are -”

- Proof-of-Work,
- Proof-of-Stake,
- Proof-of-Authority.

These steps are for cross-checking the validity and authenticity. Last, the study suggests using a Decentralized Network and provides an area-life example of A US fintech company named R3 trying to adopt the solutions.

The presentations and precautions of the study are so much appreciated as it provides one of the complete solutions. However, it was expected to show the way of implementation, which was not provided.

The study of Kaur et al., 2021 provides a ”General Cybersecurity Framework,” named ”NIST Cybersecurity Framework,” which mainly focuses on the prevention method from an upper view. According to them[55], there should be five main portions which are-

1. identify,
2. protect,
3. detect,
4. respond,
5. recover.

They make it a cyclic framework that will be repeated simultaneously.

The research of Rabbani et al., 2020 mainly focuses on the Islamic FinTech organizations and shows how it is so important to adopt blockchain technology in terms of Islamic Banking Systems[42]. The study provides some significant comparisons to get a clearer picture of the industry’s current and future if Blockchain can be adopted. However, the study does not provide any more precise idea about the implementation and accurate life evaluation.

Another study by Maiti Ghosh, 2021 shows a more comprehensive picture of how every cutting edge technology is connected to FinTech and IoT[57]. The study does not show a clear picture or pathway to tackle the cyberattacks in FinTech. However, it shows a fascinating diagram of neurotech and 3Ms association consisting of Man-Machine-Memory with the cutting edge technology.

The research of Hamid Lone Naaz Mir, 2017 comes up with another model which focuses focusing Forensic-Chain solely[27]. It says the Blockchain-based forensic

methodologies have higher potential and benefits, including maintaining transparency and integrity.

Another recent study by Jayalath Premaratne, 2021 suggests maintaining a strict internal level of security by implementing - Firewalling, Intrusion Prevision and Intrusion Detection Solutions (IPS/IDS), Web Application Firewall (WAF), log collection, and correlation with Security Incident and Event Management (SIEM), Digital Data Classification, Data Leakage Prevention (DLP), end-user identity management, Network Access Control (NAC), Security Operation Centre (SOC)[53].

According to Perlman, n.d. RegTech is a new sub-set of fintech that focuses on the technologies facilitating the industry and should be treated specially. The study shows a three-way method to secure the industry[35]. These are Regulation of Fintech's, Ancillary Regulation, and Regtech.

Though the study does not provide a depth solution, the broader picture has excellent potential.

The study of Crisanto Prenio, n.d. provides "The Hong Kong Monetary Authority's (HKMA's) Cybersecurity Fortification Initiative"[18]. It has mainly three sectors: Cyber Resilience Assessment Framework, the second is Professional Development Programme, and lastly Cyber Intelligence Sharing Platform.

According to "BUILDING INCLUSIVE DIGITAL PAYMENTS ECOSYSTEMS" the four challenges of making an inclusive digital payment system the main four challenges are – Managing Stakeholders, Balancing Innovation Building Trust, and Establishing a Regulatory Environment[12]. The study believes that the regulatory environment can make the industry more secure.

According to Laughter, to build a more secure transaction, INCREASED USE AND ENHANCEMENT OF LEI(LEGAL ENTITY IDENTIFIERS) can be implemented. It is mainly a unique 20-character, alphanumeric code used to create a unique transaction identity[21]. The research team is focusing more on implementing it at its production level.

9.2 Proposed Framework

The research team examined all the proposed frameworks and methods to secure fintech. However, a framework that is a complete solution starting from the very end-users to the massive infrastructure is very rare to found.

Hence the study provides the most comprehensive framework to secure everyone related to the FinTech industry. The name of the proposed framework is “FinSec Framework,” which stands for “FinTech Security Framework.” The central diagram of the FinSec framework is added in the following section.

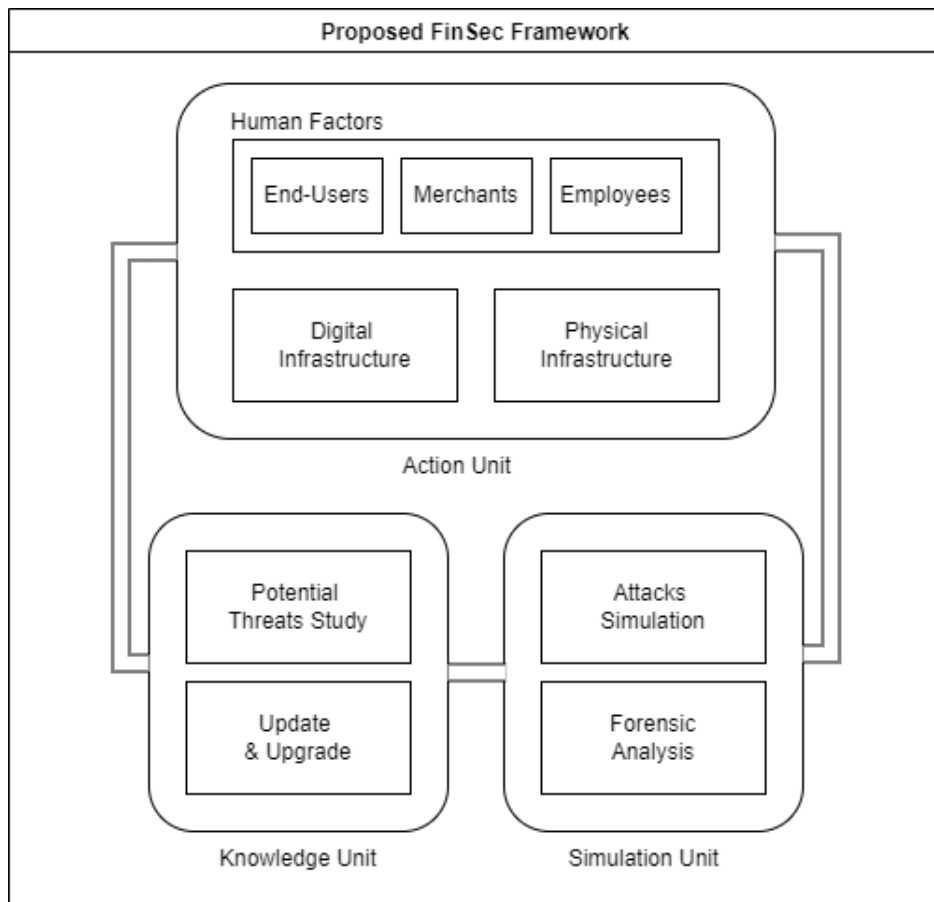


Figure 9.1: Proposed “FinSec Framework”

9.2.1 Short Description of FinSec Framework

There are mainly three different units in the framework which are sequential –

1. Action Unit,
2. Knowledge Unit and
3. Simulation unit

Again, every unit also consists of different subunits. The first unit, the action unit, contains three subunits – Human Factors, Digital Infrastructure, and Physical Infrastructure. Human factors also have three types of humans – End-Users, Merchants, and Employees of the financial organizations.

Additionally, the knowledge unit has two sub-units named Potential Threats Study and Update Upgrade sub-units. Lastly, the simulation unit contains sub-units named – Attacks Simulations and Forensic Analysis.

In terms of the work process of the framework, the action unit is the core part of the overall framework. The framework first secures the action unit using different methodologies to secure the physical and digital infrastructure and train the Human factors.

After securing the action unit, the knowledge unit keeps researching potential threats for future cyberattacks and update or upgrade the system according to the result.

Lastly, the simulation unit is dedicated to attacking simulation and penetration testing. Nevertheless, even after ensuring every level of security, if damage happens due to cyberattacks, a dedicated sub-unit forensic analysis is here to report and research the incident.

There are intercommunication tunnels between all three significant units to share knowledge between units and always keep the security patches up to date and ready to tackle any cyberattacks.

The following sections briefly describe all the units and sub-units of the proposed FinSec Framework.

9.3 Action Unit

The action unit is the core part of the proposed FinTech Security Framework. If it is closely observed, it would be clear that there are mainly three major factors related to the industry. The research team says it as –

- Human Factors,
- Digital Infrastructure factors and
- Physical Infrastructure factors

9.3.1 Human Factors

These are three types of users who are related to the industry. The following sections briefly describe the Human factors in the following section –

End-Users

The persons who are the consumers of any fintech product can be classified as end-users. For example, in Mobile Financial Services, the users of bKash, Nagad, Rocket,

and Paytm can be classified in this category. In terms of typical banking, all the users who save, transfer, and use the bank's services can also be classified.

Agents/ Merchants

The persons working as the middleman between financial service providers and the consumers can be classified in this category. For example, the persons who provide cash-out services in terms of mobile banking and those who offer very few banking facilities in agent banking hubs.

Employees

Employees are the humans who work directly with any financial organization. For instance, every single employee of a bank is categorized in this section regardless of job post and title. It is because even a single mistake by a non-technical person can open the door to breaching the bank.

9.3.2 Securing Human Factors

The research team encourages the organizations to adopt the existing security guidelines discussed in the previous sections. However, the research team believes that the existing and proposed solutions are not enough as these have been followed for a long. Hence, the research team proposes innovative solutions to make the industry more secure.

General Recommendation for End-Users

To prevent web spoofing, organizations should use encrypted authentication. Pattern authentication should be integrated with graphical models, and real-time authentication procedures should be implemented to protect against offline and online spoofing attacks.

Internet banking consumers need constant instruction on how to make secure online payments. If basic security training is conducted concurrently for the end-users, security measures will be implemented more efficiently. It would increase client trust and confidence in the security measures.

Organizations need to develop an enterprise-wide fraud control strategy that supports compliance and risk management initiatives. The IT infrastructure must provide enterprise-wide, real-time, cross-channel management and monitoring. A blockchain-based updated security framework is essential for effective fraud governance, regulations, and policies, especially in combating fraud committed through online portals. Financial institutions should establish fraud prevention programs using digital forensic auditors.

To make secure online transactions, end-users should take the following actions while using internet banking.

Fundamental Safety Standards for End-Users

The following steps are suggested to take the to increase the security of online transactions when using Internet banking:

Before Making Online Transections

- Ensure that an updated firewall and anti-virus software protect the computer.
- Ensure that the computer is spyware-free by installing anti-spyware software.
- Get the most recent security patch updates for the browser and operating system.
- Make sure the computer can download and install these updates automatically.
- Configure the browser to receive security notifications and monitor online threats at their highest level. Usually, the security settings are not enabled by default.
- Do not save any passwords and PINs on in computer or share them with anyone and use a password manager.

While Performing Online Financial Transactions

- Do not provide personal information or passwords to unsolicited phone calls or emails. Banks or police would never request PINs or online banking passwords.
- While accessing the online banking site through a web browser, always type the bank's URL into the address bar.
- Never provide personal information after visiting a website when getting a link from an anonymous email.
- The login pages of bank websites are encrypted; therefore, be sure the browser window has a secured padlock or an unbroken key mark when entering the bank's website. When a secure connection is established, the initial portion of a bank's URL will change from "HTTP" to "HTTPS."
- Whenever logged into the online account, never leave the computer unattended.
- Double-check the account numbers and security codes before making an online payment; it may be difficult to retrieve the funds if the payment is made to an incorrect recipient.

After Completing Online Banking

- If using a shared computer, be aware of logging out from all bank accounts before turning off the computer.
- Ensure that bank statements are reviewed thoroughly regularly. Inform the bank immediately if anything unusual appears on the account.

Secure Online Shopping and Safe Payments

To reduce the risk of being a victim of cyber fraud, users should follow these steps:

- Remember that bank card information may be as precious as cash in the wrong hands, so keep it safe and do not allow it to leave on site.
- When purchasing online, make sure the payment card is verified by Visa or Mastercard secure code. By integrating, the payment card will have an extra layer of protection, which prevents consumers from becoming victims of online fraud.
- Only purchase products from online sites that offer an SSL certificate. Be aware that bank websites are encrypted, and while accessing the bank site, ensure that the browser window has a secured padlock or an unbroken key symbol. A lock icon may appear in the URL bar to indicate that a website has an extra layer of security measures.
- Always keep the passwords and PINs private. Do not share them with anyone or send them through social media.
- Keep a copy of the retailer's receipt and payment details. While placing and paying for any order, keep terms and conditions and policy regarding the refund. It may be challenging to reverse an international purchase, but the user can get assistance from a payment card provider by collecting all the necessary information.
- If authorizing a series of payments or a single payment, ensure that users must understand the terms of the agreement. It may be best to use a specific credit card for online transactions.

Particular precautions to follow

- Personal information such as identities, passwords, pins, user names, account numbers, or banking card information should never be sent to third parties. If someone is concerned about the unsolicited email, contact the organization directly.
- Do not click on links in unsolicited emails that take users to a website that is not recognized. Moreover, never copy and paste a link directly from an email into the browser. Phishers may make the links seem to lead someplace while directing the users to another site. Try to use a different browser to manually enter the business's web address.
- Pop-up windows should be avoided at all costs. Sometimes, phishers will send to a legitimate company's website, but an illegal pop-up screen produced by the fraudster would appear, requesting the personal information. This form of phishing assault may be prevented by installing software that blocks pop-ups. When entering personal information on a reputable company website, look for evidence that the site is safe and has an SSL certificate.

- Create intelligent passwords for computers and make sure the passwords are unique by including letters, numbers, and symbols. Each account should have a unique password, updated every three months (90 days), and do not use the same password for other sites.
- Never use any public networks or public wifi for internet banking.
- Shred or rip any confidential information into tiny parts before destroying any confidential information.
- Be wary about disclosing any personally identifiable information, for example, the user's date of birth, in forums or on social sites such as Facebook.
- Never discard a computer or other device containing personal information without first deleting all sensitive information.
- Set up SMS alerts on the bank accounts to be notified of any unusual activity. Immediately contact the bank if the user observes any suspicious behavior on the account.
- Finally, everyone must take action to spread awareness about cybercrime and threats to their friends, family, and colleagues. The more this information is spread, the more people will be able to get knowledgeable and defend themselves.

Maximizing Communication

The research team refers to maximize the communication with the help center in order to establish a secure Fintech ecosystem. To do that, the team refers to cross-checking the information of the transaction via the support center's phone call while any end-user wants to send money of more than ten thousand BDT to any new number which has no transaction history.

Public Database

A public database where all the scammers, frauds, phone numbers, emails, and other information should be stored is necessary to identify attackers. Any human factor can submit the form if he is scammed or knows about the scammers. Then the information would be stored in the database after checking.

Scam Detection Application

The research team also suggests that individual financial organizations publish "Scam Detector Application." Moreover, the app should detect any phone call and text message if it is found in the public or Internal database flagged as scammed. There are so many spam detector applications, but nothing dedicated to fintech and published officially by financial organizations.

Licensed Merchant/ Agent

Nowadays, anyone who has a trade license can register as a merchant of any MFS in Bangladesh. The requirements of registering as an agent are lesser. Hence, the lack of knowledge of merchants is another big reason for facing scams or cyberattacks. The team proposes to make sure someone has a minimum ground-level knowledge to tackle common scams and frauds before registering as a merchant.

However, because of the massive number of merchants, it cannot be implemented overnight. Thus, MFS organizations can mark the shop of the licensed merchant to encourage end-users to get service from there.

Mandatory Security Exam

Even if non-technical “Authorities do it,” a single mistake can cause massive harm. Hence, while recruiting employees in Financial Organizations, candidates must undergo a standard security examination to secure themselves from being scammed, spammed, or attacked.

Awareness

The research team cannot neglect the importance of awarding all the “Human Factors” about the standard attacks and methodology and how they can be prevented.

9.3.3 End-User Training Model

The risk and fraud management program is compatible with the organization’s customers’ cyber safety. It may be designed to meet regulatory standards which prevent consumers from becoming victims of online fraud. The training program must include risk management instruction relevant to all types of basic security knowledge for users. With this type of framework as a guide, fintech may tailor risk management and fraud awareness programs for customers to improve their security.

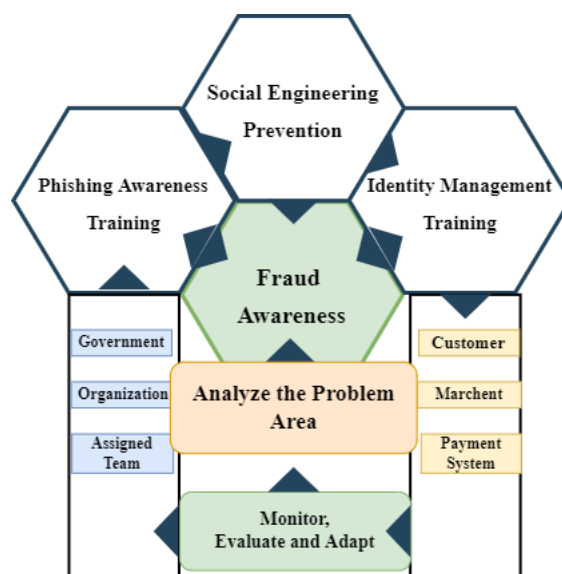


Figure 9.2: End-User Training Model

9.4 Digital Infrastructures

Digital infrastructures refer to all the applications regardless of the web, mobile, or desktop clients for both end-users and internal users related to the financial organizations. Ensuring the security of digital infrastructures is the main task to secure the whole FinTech industry. Thus, there are so many existing and proposed security frameworks implemented nowadays. The research team mentions potential security methods and frameworks in the previous sections and tries to discover the advantages and drawbacks. Along with the standard best practices, the study proposes the following methods for ensuring the security of Digital Infrastructures.

9.4.1 Securing Digital Factors

3WA

To secure the end-users from the scammers and a thousand of their phishing attacks, the research team proposes a “Three-Way Authentication,” 3WA, to make any successful transactions.

The following diagram shows how 3WA can be implemented in any application –

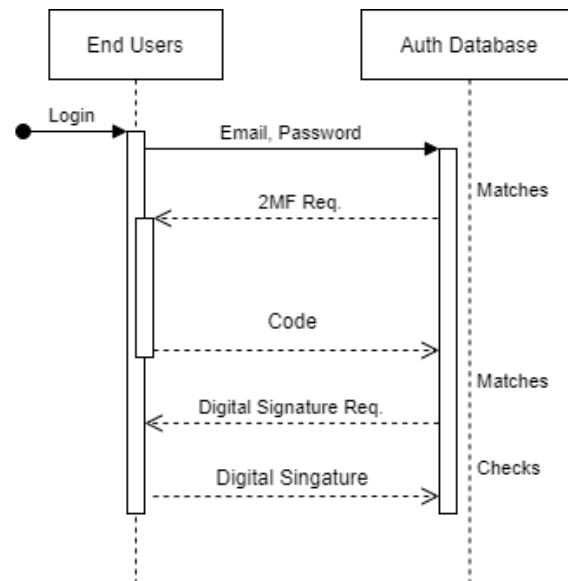


Figure 9.3: 3WA Auth

To implement 3WA, a digital signature is required, which can be the answer to a question or a voice note, or any single word or phrase. Whenever someone opens an account, he should be asked to choose a category of digital signature; then, he would input it as instructed, and the given signature will be stored in the auth database. It is suggested to store the signature as the hash value.

The research team tries to implement 3WA in existing systems. In terms of the most used Mobile Banking System in Bangladesh, if someone wants to send money, he is required to input something in the reference (USSD) field. This reference field can be turned into the digital signature field.

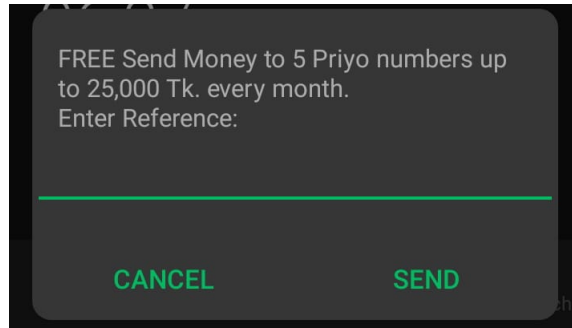


Figure 9.4: A renowned MFS's Reference

Some of the best freelancing platforms currently use the same methodology but for a different purpose.

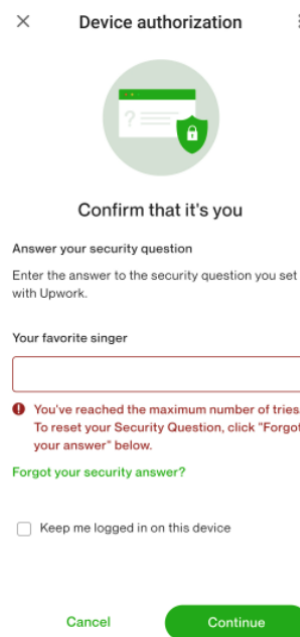


Figure 9.5: Security Question

For now, it asks a question to check the device authorization and whenever someone newly tries to access the billing section. However, a text-based digital signature is more prominent as it can be done regardless of any device, including intelligent and featured phones.

In terms of regular banking, most banks ask security questions for the same reason as Upwork. Additionally, they store the data to recover the account if it gets locked someday.

Here is a screenshot collected from the instruction pdf of a renowned Bank, where security questions are asked.

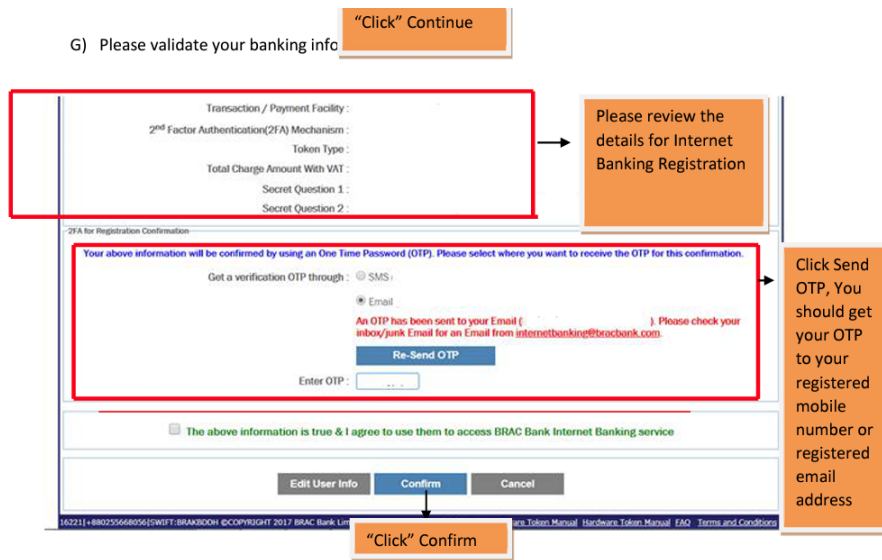


Figure 9.6: Security Questions of a renowned bank

Some bank uses the RSA key while transferring money. However, the research team highly recommends making this field required as a “Digital Signature” while making any transaction. The team believes that even if an attacker bypassed 2 step-authentication using the latest techniques, it would be almost impossible to bypass – the password, authentication, and digital signature.

3WA API

The research team also suggests using the previously mentioned 3WA method while requesting an API. For instance, when someone is trying to pay via a third-party payment gateway like SLLCommerz, it asks for OTP and pins code. Moreover, it would be almost impossible for an attacker to breach OTP, pin code, and the digital signature called 3WA.

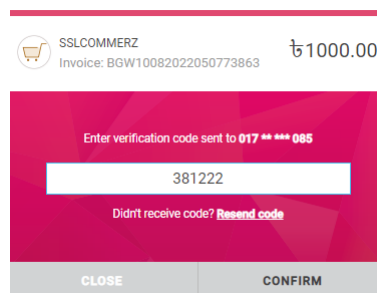


Figure 9.7: A renowned MFS’s payment via SSLCommerz (OTP)

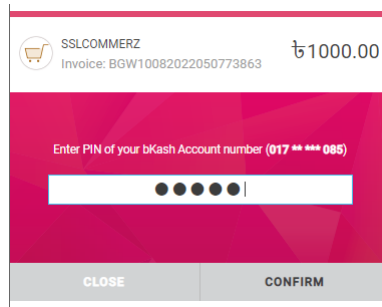


Figure 9.8: A renowned MFS’s payment via (Pin code)

Gamification

The research team proposes a gamified approach to security training for the end-users, specially MFS users in Bangladesh. It is also proposed that if an end-user successfully passes the security training, 3WA will be optional for the user. The following diagram shows a basic idea of gamification to secure the community

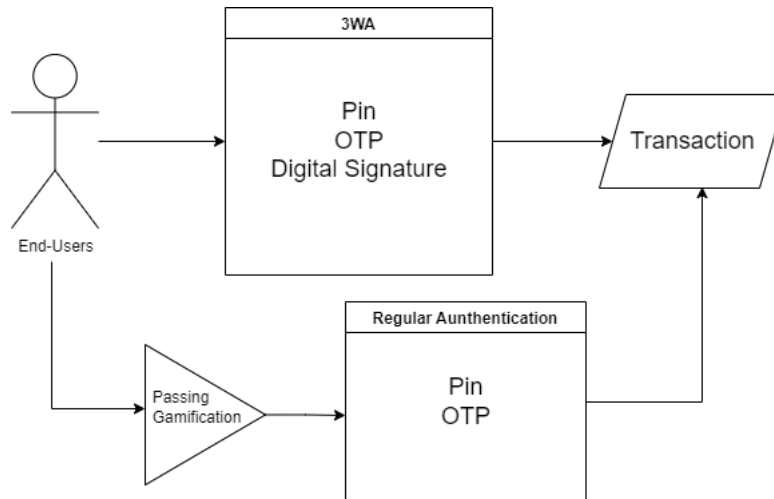


Figure 9.9: Gamification to pass 3WA

Operation-Based OTP

The research team highly suggests sending "Operation-Based OTP" from the back-end to the end user’s mobile phone. The OTP message never says about the operation that will be done after inputting the OTP. Any backend system only sends the OTP and the duration of validation of the OTP in the OTP message. It also suggests not to share the OTP with anyone in any circumstances in the OTP message. However, an OTP text never says about the operation.

Nevertheless, if the backend system can inform about the operation after inputting the OTP, it can also send the information of the financial activity when the OTP is required; then, the user would get a precise idea of what is going to happen after submitting the OTP.

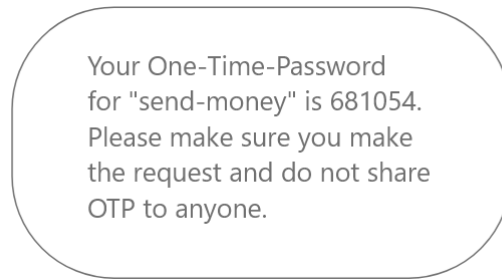


Figure 9.10: Example of proposed operation-based OTP text

Memorable Information for Third Party Authenticator

The study finds that even though people use highly secure third-party authenticators, the application cannot assure security if the device is somehow hacked. So, the research team suggests inputting some of the digits from the auto-generated third-party authenticator's array of numbers. The digit's position will be dynamically asked so any bot cannot breach the system so quickly even though it gets the code.

9.4.2 Hyperledger Fabric

Ledger Technology (DLT) for any Enterprise. The key reason to choose the platform for financial organizations as it is created on the top of blockchain and has some of the essential features required by any fintech organization. Again, the significant advantages of Hyperledger Fabric are discussed here –

- **Modular Architecture**

The most significant benefit of using Hyperledger fabric is "Modular Architecture." Hence, different departments of any financial organization can use the architecture to work together with data integrity and confidentiality.

However, the architecture has a bright future if it can be implemented in the country's Central Bank or even in the central SWIFT (Society for Worldwide Interbank Financial Telecommunications) system.

However, this research strongly recommends using the platform in all financial organizations.

The following diagram in the next section shows a basic idea of the proposed method. Here, an organization can be treated as a "Bank," and a center can be treated as a central bank. On the other hand, in terms of a single company, an organization can be treated as a "Department," and central can be treated as the company.

- **Permissioned Membership**

Hyperledger provides permission-based membership, which can be utilized in traditional banking systems whether someone newly creates an account.

- **Other Benefits**

Data on request, rich queries, and protected digital keys are other benefits of using the platform.

Currently, Amazon, Amazon Web Services (AWS), Walmart, Hitachi, and many big companies are using Hyperledger Fabric for their purposes. However, using Hyperledger fabric in FenTech is necessary to create a more secure environment.

According to some sources, some of the big giants like Paypal and Visa are using

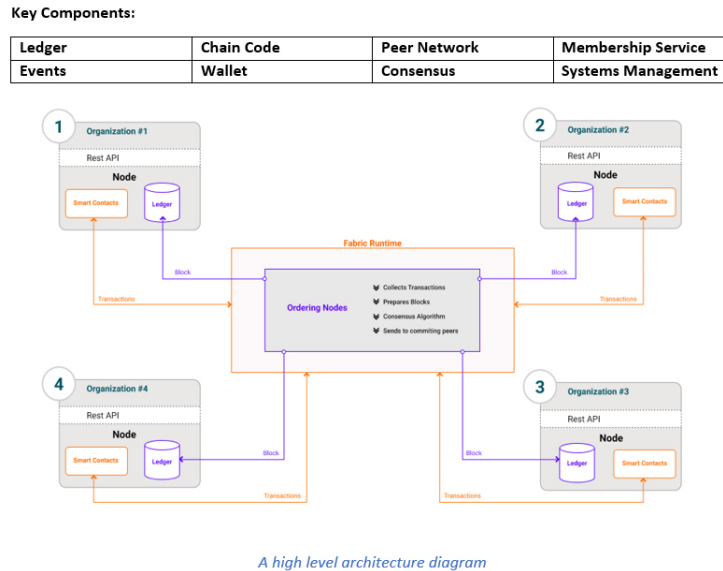


Figure 9.11: Hyperledger Fabric Architecture; Source: jktech.com

this technology. Nevertheless, the way they are using that is not available publicly because of security concerns. So, the real-world implementation of Hyperledger Fabric is already tested and ready to perform in any financial organization. In terms of Bangladesh, Standard Chartered Bank[38], HSBC Bank[64], and Prime Bank[66] are using blockchain for LC or Letter of Credit. Upay, comparatively new MFS in Bangladesh announced they are using blockchain in their app[23].

9.4.3 Hybrid Cloud

The risk of using only the public cloud for any financial system is alarming, as discussed previously. Again, using only a private cloud excludes getting the higher benefits of using a cloud.

Hence, the study proposes to use a hybrid cloud to build robust, secure, and comprehensive Digital Infrastructure for financial organizations. The research team proposes to keep Hyperledger Fabric Blockchain implementation in a public cloud-like IBM, AWS, Azure, or GCP. Moreover, the research team suggests keeping persistent volume and other confidential data like digital signatures and user details in the private cloud for better security purposes.

Here is a diagram of the proposed hybrid cloud –

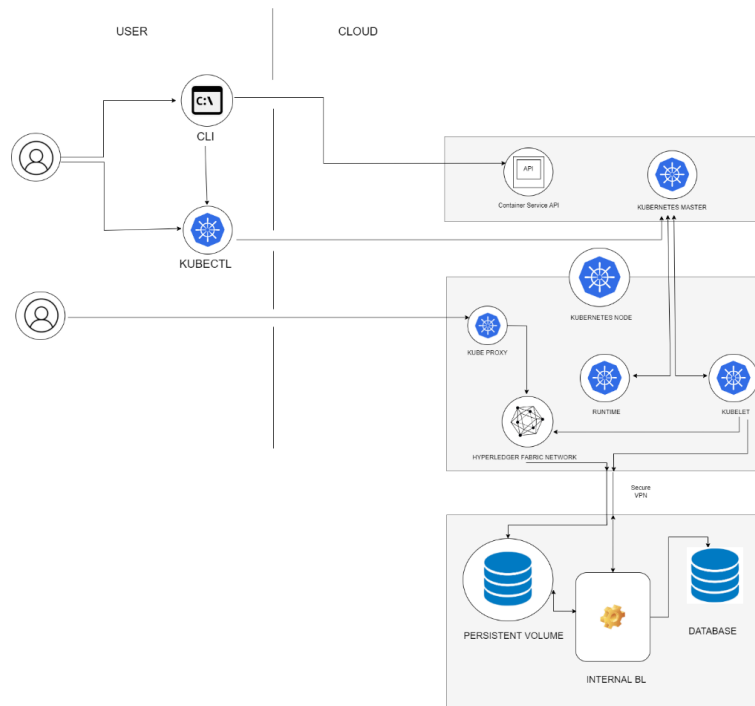


Figure 9.12: Hybrid Cloud with Hyperledger Fabric (Edited from IBM Documentation)

9.5 Physical Infrastructures

Though in the proposed hybrid cloud architecture, the security of cloud devices relies on the cloud provider; however, security of physical devices in private, on-premises cloud and all the devices of any employees are mandatory to protect from any cyber-attacks. The research to acknowledges the existing security methods for protecting physical infrastructures. Moreover, the study emphasizes the following ones –

9.5.1 Securing Physical Factors

Authorized Vendor

The first and foremost task is to buy any devices only from the authorized vendors, even if it is a single modem or printer for any sub-branch of the Bank. Every device's authenticity should be checked twice before using it. Because there are so many case studies that show the “gate” opened for the attackers because of unauthorized devices and systems. The suggestion is also the same for any OS or software.

NGFW

NGFW or Next-Generation Firewalls protects devices and networks by implementing application monitoring, awareness and controls, integrated prevention, and special threat intelligence dedicated to a cloud platform. These features are not available regular firewall.

NGIPS

NGIPS refers to “Next Generation Intrusion Prevention System” which protects devices and networks from various known-unknown, zero-day threats. Hence, it is also highly recommended.

Insider Threats

A financial company cannot make it fully secure without getting rid of insider threats. Hence, the company should always keep serious concern regarding this issue.

9.6 Knowledge Unit

The knowledge unit is the research and development unit of the proposed framework. The research team believes that it is almost impossible to keep the security framework up to date without having a dedicated knowledge unit.

Knowledge Unit consists of –

- Potential Threats Study and
- Upgrade Update

9.6.1 Potential Threats Study

Cyber attackers or scammers have colossal time to learn about different cyber-attacks outside of the country. They are more intelligent; they try different methodologies to breach confidential data and steal money.

This is why the research team highly recommends establishing a dedicated team that will mainly study the trending cyber-attacks and case studies to take precautions before getting attacked.

9.6.2 Upgrade and Update

According to the outcome of the threat analysis, the research team suggests implementing an upgrade to the system. It is also suggested to update only those patches which passed all the test cases.

9.7 Simulation Unit

The knowledge unit is the research and development unit of the proposed framework. The research team believes that it is almost impossible to keep the security framework up to date without having a dedicated knowledge unit.

Knowledge Unit consists of –

- Attacks Simulation
- Forensic Analysis

9.7.1 Attacks Simulation

One of the most significant issues with Bangladeshi Financial organizations is that few organizations have a dedicated security team. Let alone someone who can conduct black-box attacks simulation to test the system and employees' capabilities. The research team highly suggests creating a secret pen testing team to evaluate the knowledge of the employees and the current security status of the system. It is recommended to regularly make these sorts of "Black-Box attacks" so employees cannot take extra precautions before the test days. After completing every event, the organization should take steps to update the systems failures and knowledge of employees.

The team also should work as the defender to respond in the time when a company experience any actual attacks.

9.7.2 Forensic Analysis

According to Edward Snowden, American author and former computer intelligence consultant, "The best way not to be hacked is not to go online." The words show that if someone is online or connected to a network, it is not impossible to be hacked. Hence, while managing the vast digital and physical infrastructures and massive human factors, it is not impossible to experience damages or attacks in any portion. So, a forensic team must analyze the failures or problems and the footprint of the attacks.

The following diagram shows the minimal way of creating a security team for any financial organization. The research team suggests at least creating a security team consisting minimum of one person in each sub-group.

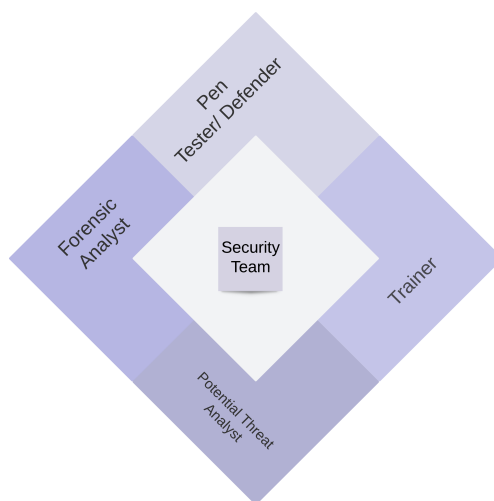


Figure 9.13: Proposed Security Team

Chapter 10

Implementation

Among all three core units – Action Unit, Knowledge Unit, and Simulation Unit, the research team implemented core features of the Action Unit.

To implement the first portion of the action team, the research team must implement three-way authentication. The team initially implemented the OTP-based login using Firebase as backend and ES6 as frontend, HTML, and CSS.

After successfully implementing the OTP, the user will input the digital signature. The user's favorite book's name and author are asked for the test demonstration as the digital signature.

Lastly, the end-user must provide an email password to complete 3WA authentication.

The research team also demonstrated Gamification by showing some scenarios along with illustrations so that users could relate to him. Then the user was asked to answer the question based on the scenario.

Finally, the user will learn about his knowledge of phishing and social engineering by finding how many questions and answers he has given. The user can also retake the quiz Gamification.

The research team also demonstrated Hyperledger Fabric-based simple financial application. The group added necessary docker images in the local repository and followed the documentation to complete the task. The basic demo application has three organizations and one endorser. All the organization has one distinct peer.

All the codebases and complete demonstration are found in the following GitHub link - <https://github.com/users/teamjaf/projects/3/views/1> or [Click Here](#).

10.1 Analysis

The following table shows how the framework protects end-users and organizations from different cyber-attacks.

Attacks	Which part of FinSec is protecting?	How is that part protected?
OTP bypassing, sim/ phone cloning	3-Way Authentication	The attackers cannot get access using the mentioned attacks even though he bypasses email-password and OTP. He would not be able to bypass the digital signature of 3WA.
Spear Phishing, Smishing, Vishing	Gamification of Human Factor	As our gamification will train the users, the risk of phishing will be decreased. Again, no one will be influenced by any wrong instruction or message in terms of Bypassing by gamification unit.
Reconnaissance	Gamification of Human Factor	Gamification makes user concerned about personal information and prevents them from their data leakage.
Credential Harvesting/ Account Harvesting	Gamification of Human Factor	Gamification can prevent users from protecting their data.

Table 10.1: Preventing Attacks

Attacks	Which part of FinSec is protecting?	How is that part protected?
Pharming	Hyperledger Fabric of Digital Infrastructure	As FinSec uses Hyperledger Fabric for network establishment, no one can access the network without permission. So hackers cannot manipulate the traffic within that network.
Dumpster Diving	Hyperledger Fabric and Hybrid Cloud of Digital Infrastructure	The network will be safe as this research proposed establishing a hyper ledger fabric, and data will be safe as it will keep in the hybrid cloud.
Shoulder Surfing	3WA (Three-Ways-Authentication)	As this research proposed to use 3WA (Three-Ways-Authentication) if hackers managed to break the password, it would be tough to manage the user's digital signature.
Tailgating	Gamification of Human Factor and 3WA (Three-Ways-Authentication)	Gamification helps users protect themselves from social engineering, and by chance of manipulation, 3WA (Three-Ways-Authentication) helps protect them from hack access.
Typosquatting	Gamification of Human Factor	Being trained by FinSec gamification, the chances of social engineering will be reduced as there have many fraud scenarios to pass the gamification unit.
Malware	Hyperledger Fabric and Hybrid Cloud of Digital Infrastructure	Because Hyperledger is a permission blockchain, a single affected computer cannot influence the whole network. However, if it is the admin or endorser's device, then that is very risky .

Table 10.2: Preventing Attacks

Attacks	Which part of FinSec is protecting?	How is that part protected?
Trojans	Hyperledger Fabric of Digital Infrastructure	An attacker cannot breach a modular Hyperledger architecture. Even if someone breaches the system, he cannot damage the whole network.
Remote access Attack	Hyperledger Fabric of Digital Infrastructure	Hyperledger Fabric protects the network as access to the module needs permission. So it can also protect the Trojan's access.
Worms	Hyperledger Fabric of Digital Infrastructure	Hyperledger Fabric can protect the network from malware injection as it detects any suspicious activity.
Crypto Malware	Hyperledger Fabric of Digital Infrastructure	Hyperledger Fabric ensures module security from unauthorized access.
Fileless virus	Knowledge unit and Simulation unit	Knowledge and simulation unit of FinSec framework can help identify the hackers' footprint.
Rootkit	Hyperledger Fabric of Digital Infrastructure	Hyperledger Fabric can make the network secure from this type of malware attack.
Dictionary	3WA (Three-Ways-Authentication)	Password cannot be implemented due to 3WA (Three-Ways-Authentication) as it needs a digital signature.
Overflow Attack	Hybrid Cloud	As the main target of the overflow attack is the data section, the attackers will not get a single target to utilize the attack by implementing a hybrid cloud. Again, it is very tough to simulate attacks and gain access to this architecture.
Impersonation Attack	Mandatory security exam of Human Factor	As an impersonation attack creates a fake email to breach data, security tests increase identity detection concerns.

Table 10.3: Preventing Attacks

Attacks	Which part of FinSec is protecting?	How is that part protected?
Error Handling Attack	Hyperledger fabric	This portion of our framework ensures the confidentiality of data by modular architecture.
SSL stripping	Hybrid cloud	As the Hybrid cloud controls the data, it will protect the data from unauthorized access.
API modification	3WA API	Every API login attempt will have to pass all three steps of authentication.
Evil twin	NGIPS of physical infrastructure	Next-Generation Intrusion Prevention System protects the network from various known-unknown threats, which reduces the risk of evil twin.
Shadow IT	Securing Human factor of Action unit	Employees will be well trained and aware of the Human factor unit's unsanctioned or unapproved hardware or software.
Bluesnarfing	Securing Human factor of Action unit	People will be more concerned about their connectivity and pair by acquiring knowledge about human factors.
Bluejacking	Gamification	The Gamification process trains the user to understand the proper instructions and connection, which reduces the risk of Bluejacking.
Attacks in IoT	Modular architecture of Hyperledger fabric	The modular architecture ensures the confidentiality between the module to the module, which decreases the risk of MITM.

Table 10.4: Preventing Attacks

Attacks	Which part of FinSec is protecting?	How is that part protected?
Man in the Middle Attack	Hyperledger fabric	Hyperledger provides protected digital keys, ensuring security from this type of attack.
DHCP configuration	Authorized Vendor of Physical infrastructure	Authorized Vendor filters messages and restricts traffic from unauthorized sources.
Unauthorized L3 Router	Authorized Vendor of Physical infrastructure	Every device's authenticity will be checked twice before using it, so there will be no risk from unauthorized devices.
Redirecting by using DNS Spoofing	Scam detection application of Human Factor	As cybercriminals push users to open suspicious sites to deceive and access information, Scam detection can recognize it and conduct quick reactions.
Man in the middle	Hyperledger fabric	Hyperledger provides protected digital keys, ensuring security from this type of attack.
Address Resolution Protocol	Hyperledger fabric	The modular architecture of hyper ledger fabric will enable safeguard on trusted ports.
ARP poisoning	Physical Infrastructure of Action Unit	Securing physical infrastructure will help to control physical 'access.
MAC Cloning, Flooding	Gamification	MAC cloning fools simple authentication checks, but gamification ensures more security
DoS Attack	Hybrid Cloud	A hybrid cloud will secure the network as it is more protected and secure than a public cloud.
DDoS Attack	Hybrid Cloud	The hybrid cloud protects the system from this sort of attack as it has the control and ownership of its data.

Table 10.5: Preventing Attacks

Attacks	Which part of FinSec is protecting?	How is that part protected?
STP (Spanning Tree Protocol)	Hyperledger fabric	Hyperledger Fabric provides permissioned membership, which will secure the system from redundant links.
Domain Hijacking	Memorable information for third party authenticator	Our system will dynamically ask the digit's portion of the auto-generated third party authenticator's array of numbers.
DNS poisoning	Hybrid cloud	A hybrid cloud ensures data security as a private cloud is being used here.
URL redirection	Scam detection application of Human Factor	As attackers force to visit untrustworthy links to steal and access the data, Scam detection can identify it and can take action immediately.
DNS Tunnelling	Hyperledger fabric	It will protect the data with rich queries, modular architecture, and protected digital keys.
Domain reputation	Gamification	The Gamification process ensures high-level security from data leakage.

Table 10.6: Preventing Attacks

Chapter 11

Comparison

Proposed Framework	Comparing Framework	Discussion
FinSec	NIST Framework	NIST framework is a five-cycle proposal model to secure the industry. The main difference is that NIST does not provide any dedicated training module or application level implementation method.
FinSec	COBIT	ISACA's framework is an excellent solution for Cybersecurity Governance. However, in terms of educating end-users, FinSec provides a more interactive way.
FinSec	Send-and-Subscribe Framework	Send-and-Subscribe frameworks introduce a new protocol based on the message queue. As the protocol has not yet been tested, hence FinSec steps forward.

Table 11.1: Framework Comparison

Proposed Framework	Comparing Framework	Discussion
FinSec	Forensic-Chain Framework	The potential of the Forensic-Chain Framework is promising because of using blockchain in forensic analysis. Nevertheless, the framework is not a complete solution for any financial organization where FinSec provides comprehensive solutions.
FinSec	HKMA Framework	The Hong Kong Monetary Authority's(HKMA's) Cybersecurity Fortification Initiative emphasizes almost every industry sector; however, it does not provide any precise observation on application development.

Table 11.2: Framework Comparison

Chapter 12

Drawbacks

The main drawback of the framework is that ensuring such a robust and comprehensive framework is costly. An organization needs to ensure so many tasks to get this kind of perfection. A good number of applications need to develop for the end-users.

Again, maintaining hybrid cloud architecture and Hyperledger fabric is not easy for the existing organizations. Nevertheless, creating a minimalistic security team can be done overnight. Later on, the research team suggests implementing the 3WA method first, then publishing applications targeting end-users and organizing training for all human factors. Finally, updating the existing system into a hybrid cloud-based Hyperledger's blockchain platform. Moreover, it will take a little longer while ensuring this security level for a successful transaction. However, a few seconds or steps can ensure end-users do not lose their hard-working money.

Even if it is costly, it will save from massive financial and organizational damages which cannot be recovered most of the time. So, precaution is always better than prevention, and the research team highly encourages all the financial organizations to ensure the proposed framework, "FinSec," in their organizations.

Chapter 13

Future Work

The research team will launch its basic security training for end-users in future work, which was discussed in the previous section.

Additionally, the researchers are willing to provide licenses for the merchants and agents. Moreover, the team intends to dedicate certification to non-technical and technical employees of any financial organization.

However, the research team is mainly focused on developing an open-source “Fin-Sec Framework” with proper documentation so that any financial organization can adopt the framework most easily. The team is also researching to develop its open-source project implementation in the proposed hybrid cloud-based Hyperledger fabric blockchain solution.

Chapter 14

Conclusion

To reiterate, Cyber Threats and Scams are a critical concern in the virtual world, affecting nearly every financial sector linked to the Internet since transactions now take place in a fraction of a second. As new technology increases the pace at which companies and their users overgrow, the likelihood of any cyberattack on FinTech organizations, including mobile banking, is very high. Consequently, cyber-attacks like DoS and DDoS attacks, MITM attacks, Phishing attacks, Ransomware, and other emerging threats make people, including service providers and consumers, more vulnerable.

Through social engineering, hackers target the naive; clever people also use it to fall into this trap, which presents a significant issue. Appropriate measures should be implemented to make the financial sector safer, including Blockchain solutions. Prevention is the most effective answer for cybercrime today, and we can do our best to bring that solution to reality.

Bibliography

- [1] E. Georgiadou, “Marshall McLuhan’s “global village” and the internet,” *Canterbury, Yayınlanmamış Yüksek Lisans Tezi. doi*, vol. 10, 1995.
- [2] L. Kleinrock, “An early history of the internet [history of communications],” *IEEE Communications Magazine*, vol. 48, no. 8, pp. 26–36, 2010.
- [3] C. Möckel and A. E. Abdallah, “Threat modeling approaches and tools for securing architectural designs of an e-banking application,” in *2010 Sixth International Conference on Information Assurance and Security*, IEEE, 2010, pp. 149–154.
- [4] D. Kriz, “Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity,” in *2011 Second Worldwide Cybersecurity Summit (WCS)*, IEEE, 2011, pp. 1–3.
- [5] *Case study - gsma*, Jan. 2013. [Online]. Available: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/Case_Study_-bKash.pdf.
- [6] G. K. Juneja, “Ethical hacking: A technique to enhance information security,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 2, no. 12, pp. 7575–7580, 2013.
- [7] M. Lagazio, N. Sherif, and M. Cushman, “A multi-level approach to understanding the impact of cyber crime on the financial sector,” *Computers & Security*, vol. 45, pp. 58–74, 2014.
- [8] G. N. Reddy and G. Reddy, “A study of cyber security challenges and its emerging trends on latest technologies,” *arXiv preprint arXiv:1402.1842*, 2014.
- [9] K. Gai, M. Qiu, H. Zhao, and W. Dai, “Anti-counterfeit scheme using monte carlo simulation for e-commerce in cloud systems,” in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, IEEE, 2015, pp. 74–79.
- [10] J.-O. Park and B.-W. Jin, “A study on authentication method for secure payment in fintech environment,” *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 15, no. 4, pp. 25–31, 2015.
- [11] Star Business Report, “Bangladesh Vulnerable to Cyber Attacks,” May 2015. [Online]. Available: <https://www.thedailystar.net/business/bangladesh-vulnerable-cyber-attacks-73048>.

- [12] *BUILDING INCLUSIVE DIGITAL PAYMENTS ECOSYSTEMS: Guidance Note for Governments*, 2017. [Online]. Available: https://www.gpfi.org/sites/gpfi/files/documents/GPFI%5C%20Guidance%5C%20Note%5C%20Building%5C%20Inclusive%5C%20Dig%5C%20Payments%5C%20Ecosystems%5C%20final_0.pdf.
- [13] M. Aaron, F. Rivadeneyra, and S. Sohal, “Fintech: Is this time different? a framework for assessing risks and opportunities for central banks,” Bank of Canada Staff Discussion Paper, Tech. Rep., 2017.
- [14] S. Ambore, C. Richardson, H. Dogan, E. Apeh, and D. Osselton, “A resilient cybersecurity framework for mobile financial services (mfs),” *Journal of Cyber Security Technology*, vol. 1, no. 3-4, pp. 202–224, 2017.
- [15] *An Impact Study on Mobile Financial Services (MFSs) in Bangladesh-”A Joint Research by Bangladesh Bank and University of Dhaka”*, Dec. 2017. [Online]. Available: https://www.bb.org.bd/pub/special/impact_mfs_27092018.pdf.
- [16] M. Bishop, D. Burley, S. Buck, J. J. Ekstrom, L. Fitcher, D. Gibson, E. K. Hawthorne, S. Kaza, Y. Levy, H. Mattord, *et al.*, “Cybersecurity curricular guidelines,” in *IFIP World Conference on Information Security Education*, Springer, 2017, pp. 15–16.
- [17] J. C. Crisanto and J. Prenio, *Regulatory approaches to enhance banks’ cybersecurity frameworks*. Bank for International Settlements, Financial Stability Institute, 2017.
- [18] ———, *Regulatory approaches to enhance banks’ cyber-security frameworks*. Bank for International Settlements, Financial Stability Institute, 2017.
- [19] B. O. Emeka and S. Liu, “Security requirement engineering using structured object-oriented formal language for m-banking applications,” in *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, IEEE, 2017, pp. 176–183.
- [20] M. S. Islam, S. A. Eva, and M. Z. Hossain, “Predicate offences of money laundering and anti money laundering practices in bangladesh among south asian countries.,” *Studies in Business & Economics*, vol. 12, no. 3, 2017.
- [21] J. Langthaler and J. L. Niño, *An overview on de-risking: Drivers, effects and solutions*, 2017.
- [22] A. A. Shaikh, P. Hanafizadeh, and H. Karjaluto, “Mobile banking and payment system: A conceptual standpoint,” *International Journal of E-Business Research (IJEER)*, vol. 13, no. 2, pp. 14–27, 2017.
- [23] Star Business Desk, “UCB launches digital banking platform Upay,” Oct. 2017. [Online]. Available: <https://www.thedailystar.net/business/ucb-launches-digital-banking-platform-upay-1477891>.
- [24] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, “A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate,” *Journal of Cybersecurity*, vol. 4, no. 1, ty006, 2018.
- [25] J. Callen-Naviglia and J. James, “Fintech, regtech and the importance of cybersecurity.,” *Issues in Information Systems*, vol. 19, no. 3, 2018.

- [26] J. Coetzee, “Strategic implications of fintech on south african retail banks,” *South African Journal of Economic and Management Sciences*, vol. 21, no. 1, pp. 1–11, 2018.
- [27] A. H. Lone and R. N. Mir, “Forensic-chain: Ethereum blockchain based digital forensics chain of custody,” *Sci. Pract. Cyber Secur. J*, vol. 1, pp. 21–27, 2018.
- [28] P. Seemba, S. Nandhini, and M. Sowmiya, “Overview of cyber security,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 11, pp. 125–128, 2018.
- [29] *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Sep. 2019. [Online]. Available: <https://ieeexplore.ieee.org/xpl/conhome/8954489/proceeding>.
- [30] Astya, P. N., Singh, M., *IEEE 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Oct. 2019. [Online]. Available: <https://ieeexplore.ieee.org/xpl/conhome/8966553/proceeding>.
- [31] *Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations*, Sep. 2019. [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/banks-under-attack-tactics-and-techniques-used-to-target-financial-organizations>.
- [32] S. Fernandez-Vazquez, R. Rosillo, D. De La Fuente, and P. Priore, “Blockchain in fintech: A mapping study,” *Sustainability*, vol. 11, no. 22, p. 6366, 2019.
- [33] N. Joveda, M. T. Khan, A. Pathak, and B. Chattogram, “Cyber laundering: A threat to banking industries in bangladesh: In quest of effective legal framework and cyber security of financial information,” *International Journal of Economics and Finance*, vol. 11, no. 10, pp. 54–65, 2019.
- [34] Y. Namestnikov, *Cybercriminals vs financial institutions in 2018: What to expect*, Oct. 2019. [Online]. Available: <https://securelist.com/cybercriminals-vs-financial-institutions/83370/>.
- [35] L. Perlman, *Fintech and regtech: Data as the new regulatory honeypot*, 2019.
- [36] A. Saravanan and S. S. Bama, “A review on cyber security and the fifth generation cyberattacks,” *Oriental Journal of Computer Science and Technology*, vol. 12, no. 2, pp. 50–56, 2019.
- [37] Y. . Wardad |, “Cyber attacks continue to rise in bangladesh,” *The Financial Express*, Feb. 9, 2019. [Online]. Available: <https://thefinancialexpress.com.bd/sci-tech/cyber-attacks-continue-to-rise-in-bangladesh-1549427552>.
- [38] M. Hasan, “StanChart executes Bangladesh’s first-ever blockchain LC transaction,” Aug. 2020. [Online]. Available: <https://www.thedailystar.net/business/news/stanchart-executes-bangladeshs-first-ever-blockchain-lc-transaction-1945733>.
- [39] M. B. Imerman and F. J. Fabozzi, “Cashing in on innovation: A taxonomy of fintech,” *Journal of Asset Management*, vol. 21, no. 3, pp. 167–177, 2020.
- [40] (Dec. 16, 2020). “Malicious domain in solarwinds hack turned into ‘killswitch’,” [Online]. Available: <https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/>.

- [41] S. Mehrban, M. W. Nadeem, M. Hussain, M. M. Ahmed, O. Hakeem, S. Saqib, M. M. Kiah, F. Abbas, M. Hassan, and M. A. Khan, “Towards secure fintech: A survey, taxonomy, and open research challenges,” *IEEE Access*, vol. 8, pp. 23 391–23 406, 2020.
- [42] M. R. Rabbani, S. Khan, and E. I. Thalassinou, “Fintech, blockchain and islamic finance: An extensive literature review,” 2020.
- [43] K.-E.-K. (Babu), “Cyber Security in the Global Village and Challenges for Bangladesh: An Overview on Legal Context,” *Cybersecurity, Privacy and Freedom Protection in the Connected World*, pp. 253–267, 2021. DOI: 10.1007/978-3-030-68534-8\{_\}16.
- [44] E. Abad-Segura, A. Infante-Moro, M.-D. González-Zamar, and E. López-Meneses, “Blockchain technology for secure accounting management: Research trends analysis,” *Mathematics*, vol. 9, no. 14, p. 1631, 2021.
- [45] I. Aldasoro, J. Frost, L. Gambacorta, D. Whyte, *et al.*, “Covid-19 and cyber risk in the financial sector,” Bank for International Settlements, Tech. Rep., 2021.
- [46] ———, “Covid-19 and cyber risk in the financial sector,” Bank for International Settlements, Tech. Rep., 2021.
- [47] “Bangladesh lags behind in fintech ecosystem globally,” *Dhaka Tribune*, Jun. 27, 2021. [Online]. Available: <https://archive.dhakatribune.com/business/2021/06/27/bangladesh-lags-behind-in-fintech-ecosystem-globally>.
- [48] “Cyber Attacks Hit Over 200 Organizations Including Bangladesh Bank, BTRC,” Apr. 2021. [Online]. Available: <https://archive.dhakatribune.com/bangladesh/2021/04/02/cyber-attacks-hit-over-200-organizations-including-bangladesh-bank-btrc>.
- [49] T. Desk, “When North Korean hackers almost pulled off a billion-dollar heist from Bangladesh Bank,” Jun. 2021. [Online]. Available: <https://www.thedailystar.net/toggle/news/when-north-korean-hackers-almost-pulled-billion-dollar-heist-bangladesh-bank-2115317>.
- [50] “Explained: The story of how north korea hackers stole \$81 million from bangladesh bank,” *The Indian Express*, Jun. 30, 2021. [Online]. Available: <https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/>.
- [51] J. Goldberg, *Biggest Threats To Cyber Security In Banking: Safe Fintech Solutions*, May 2021. [Online]. Available: <https://innovecs.com/blog/biggest-threats-to-cyber-security-in-banking-safe-fintech-solutions/>.
- [52] S. M. M. Islam, “Mobile Financial Services: Strengthen Compliance With Anti-money Laundering, Anti-terror Financing Measures,” Jan. 2021. [Online]. Available: <https://www.thedailystar.net/mobile-financial-services-strengthen-compliance-anti-money-laundering-anti-terror-financing-measures-2029925>.
- [53] J. A. R. C. Jayalath and S. C. Premaratne, “Analysis of key digital technology infrastructure and cyber security consideration factors for fintech companies,” *International Journal of Research Publications*, vol. 84, no. 1, 2021. DOI: 10.47119/ijrp100841920212246.

- [54] L.-Y. Jiang, C.-J. Kuo, Y.-H. Wang, M.-E. Wu, W.-T. Su, D.-C. Wang, O. Tang-Hsuan, C.-L. Fu, and C.-C. Chen, “A transparently-secure and robust stock data supply framework for financial-technology applications,” in *Asian Conference on Intelligent Information and Database Systems*, Springer, 2021, pp. 616–629.
- [55] G. Kaur, Z. Habibi Lashkari, and A. Habibi Lashkari, “Designing cybersecure framework for fintech,” in *Understanding Cybersecurity Management in FinTech*, Springer, 2021, pp. 167–177.
- [56] G. Kaur, Z. H. Lashkari, and A. H. Lashkari, *Understanding Cybersecurity Management in FinTech*. Springer, 2021.
- [57] M. Maiti and U. Ghosh, “Next generation internet of things in fintech ecosystem,” *IEEE Internet of Things Journal*, 2021.
- [58] Marketing Team, *10 Facts About Social Engineering That You Need to Know*, May 2021. [Online]. Available: <https://www.graphus.ai/blog/10-facts-about-social-engineering-that-you-need-to-know/>.
- [59] —, *10 Facts About Social Engineering That You Need to Know*, May 2021. [Online]. Available: <https://www.graphus.ai/blog/10-facts-about-social-engineering-that-you-need-to-know/>.
- [60] V. Prabhu, *Security Challenges Within the FinTech Sector*, May 2021. [Online]. Available: <https://www.itproportal.com/features/security-challenges-within-the-fintech-sector/>.
- [61] R. Shevlin, “PayPal’s Domination Of Mobile Payments Is Coming To An End,” *Forbes*, Jul. 2021. [Online]. Available: <https://www.forbes.com/sites/ronshevlin/2021/07/13/paypals-domination-of-mobile-payments-is-coming-to-an-end/?sh=6793da402e6d>.
- [62] *Significant Cyber Incidents*, 2021. [Online]. Available: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- [63] G. Singh, R. Gupta, and V. Vatsa, “A framework for enhancing cyber security in fintech applications in india,” in *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, IEEE, 2021, pp. 274–279.
- [64] *Blockchain for Trade Finance*, 2022. [Online]. Available: <https://www.business.hsbc.com.bd/en-gb/campaigns/innovation-digital-transformation/blockchain-for-trade-finance>.
- [65] *Financial Institutions Data Breaches on Deep Web*, Jan. 2022. [Online]. Available: <https://socradar.io/resources/financial-institutions-data-breaches-on-deep-web/>.
- [66] *Prime Bank becomes the first Bangladeshi Bank to execute interbank blockchain LC transaction*. [Online]. Available: <https://www.primebank.com.bd/interbank-blockchain-lc-transaction/>.
- [67] (). “Timeline of cyber incidents involving financial institutions,” [Online]. Available: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline?fbclid=IwAR2F18auDz6Lx_28m6u4NiRjzVPvvLoziMJAR7zwo8cIgP-CCEm79ohTGMk (visited on 05/23/2021).

FAQ

1. What is new in the Framework?

Ans: In Bangladesh, the whole Framework is a unique combination. 3WA, 3WA API, Gamification, and operational-OTP are entirely new in the country's context.

In terms of the world, some of the features are implemented in different applications or services; however, there is nothing the same as the Framework.

2. Why are you providing a training model when we have PCI and so on?

Ans: FinSec's End-users training model does not replace PCI's standards. Instead, it is an addition to the industry focusing more on end-users to protect the industry.

3. What is the reason for using blockchain?

Ans: According to IBM, the three main reasons for implementing blockchain in the banking system are – KYC (Know your Customer), LC (Letter of Credit), and ledger system, which cannot be implemented in regular applications.

Three Bangladeshi banks use blockchain for LC – Standard Chartered Bank, HSBC, and Prime Bank.

Bangladesh Bank is also planning to utilize KYC in the blockchain.

4. One of the most consequential issues with blockchain is the privacy of each transaction; how can you encounter this?

Ans: Among the three types of blockchain, the problem occurs only in a public blockchain. However, Hyperledger Fabric is a consortium blockchain framework that is modular and permission-based. Hence, the problem does not occur in the network.

5. What is the reason for using a hybrid cloud?

Ans: To keep my data in my hands and also get the benefits of the public cloud.

6. Why are you using Hyperledger fabric?

Ans: Because of its modular and permissions architecture.

7. How are you using Hyperledger fabric in financial organizations?

Ans: There are mainly two reasons - Banking organizations want to adopt blockchain, and they do not want to adopt public blockchain like Ethereum.

8. How is Hyperledger securing in the Framework?

Ans: Hyperledger can help protect the system from the common 42 attacks

described in the previous section, which are very tough to ensure in regular architecture.

9. Are you thinking there is no chance of cyberattacks in the Hyperledger?
Ans:No. There are also some security issues with Hyperledger. Certificate authority and proper key management are the main two.
10. Are you thinking there is no chance of cyberattacks in the Framework?
Ans:No. Even though after implementing the Framework, there can be cyberattacks. However, the chance of getting damage will be so less.
11. Which components are you deploying on the public cloud?
Ans:Ingress and egress, load-balancer, virtual instances
12. Which components are you deploying on-premises?
Ans:Persistent volumes of Kubernetes and databases.
13. Why is it necessary to challenge exciting architecture whenever it is doing great expect some incidents?

Ans: The biggest problem of regular applications is that so many attack vectors can be easily implemented. Even though someone with very little knowledge can damage a lot using some tools.

On the other hand, it would be tough to create damage if the Framework can be implemented. Moreover, even though this implementation happens, the damage would be significantly less than the typical application development.