

# Preventing National Identity Forgery in Bangladesh using IGA based Security Controls

by

Afsarul Islam Meraj

18301239

Sadia Ferdous Samindra

19301274

Tasnim Fuyara Chhoan

18101575

Afsana Sharmily Kashpia

18301010

Tawhid Ahmed

18301269

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  
September 2022

© 2022. Brac University  
All rights reserved.

# Declaration

It is hereby declared that

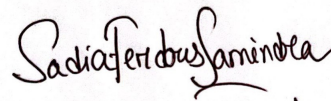
1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material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

**Student's Full Name & Signature:**



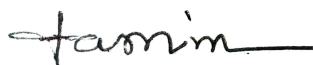
---

Afsarul Islam Meraaj  
18301239



---

Sadia Ferdous Samindra  
19301274



---

Tasnim Fuyara Chhoan  
18101575



---

Afsana Sharmily Kashpia  
18301010



---

Tawhid Ahmed  
18301269

# Approval

The thesis/project titled “Preventing National Identity Forgery in Bangladesh using IGA based Security Controls” submitted by

1. Afsarul Islam Meraj (18301239)
2. Sadia Ferdous Samindra (19301274)
3. Tasnim Fuyara Chhoan (18101575)
4. Afsana Sharmily Kashpia (18301010)
5. Tawhid Ahmed (18301269)

Of Summer, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on September 22, 2022.

## Examining Committee:

Supervisor:

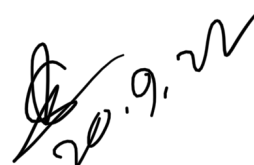


---

Dr. Md. Iqbal Hossain

Associate Professor  
Department of Computer Science and Engineering  
Brac University

Co-Supervisor:



---

Md. Arif Shakil

Lecturer  
Department of Computer Science and Engineering  
Brac University

Program Coordinator:

---

Dr. Md. Golam Rabiul Alam

Associate Professor  
Department of Computer Science and Engineering  
Brac University

Head of Department:  
(Chairperson)

---

Dr. Sadia Hamid Kazi

Head of the Department  
Department of Computer Science and Engineering  
Brac University

## Abstract

The rapid diffusion of the internet coupled with the vision of "Digital Bangladesh" has given rise to e-government services to improve the capability, accountability, and accessibility of different e-government services like E-banking, online Election Commission service, E-passport service etc. In this digital age, e-government services are quickly becoming one of the most efficient and vital practices in Bangladesh, allowing governments to communicate with businesses, people, employees, and even other government organizations. But besides these tremendous opportunities, e-services also have to face some serious security challenges, as the main factors of e-service practice and security are different from traditional government services because of the online environment. The government has to face more security threats in online services. According to a January 2018 estimate, there are roughly 17.61 lakh internet banking customers, with the majority of individuals using internet banking for fraudulent transfer operations. According to a Bangladesh Bank data report from January 2018, around 7.18 lakh transactions, totaling 2175 crore taka, were conducted over the internet banking network. Besides E-banking, E-passport and online NID services are widely used by users throughout the country. Furthermore, throughout the last two decades, security concerns in the E-service arena have received increased attention. So, we should be concerned about the security issues surrounding these services so that citizens can use online services more efficiently with the highest security possible. So, our work will be focused on the most important and sensitive E-government service, the online NID service, to find all the possible security failings or weaknesses of this service initially. After that, we will work to establish a Plug-and-Play (PnP) model to secure our systems. This model hopefully captures the E-service technology security issues in Bangladesh and the proactive measures to reduce and uproot or reduce all those security threats.

**Keywords:** IGA; National identity; Identity forgery; Identity governance; Identity Administration; online governmental services; Bangladesh; e-government; NID; eServices.

## **Acknowledgement**

First and foremost, Alhamdulillah, and by the grace of Allah, we were able to finish our thesis without too many setbacks.

After that, we are forever grateful to our supervisor, Dr. Md. Iqbal Hossain, for his unconditional help. He helped us instantly almost every time.

Then, we would like to thank our co-supervisor, Md. Arif Shakil, for his kind assistance and suggestions. He also assisted us when we required it.

Lastly, our parents, without whom it could not have been conceivable. We are currently preparing to graduate, thanks to their kind prayers and support.

# Contents

<b>Declaration</b>	<b>i</b>
<b>Approval</b>	<b>ii</b>
<b>Abstract</b>	<b>iv</b>
<b>Acknowledgment</b>	<b>v</b>
<b>Table of Contents</b>	<b>v</b>
<b>List of Figures</b>	<b>viii</b>
<b>List of Tables</b>	<b>ix</b>
<b>Nomenclature</b>	<b>x</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Research Problem . . . . .	2
1.2 Research Objectives . . . . .	3
1.3 Thesis Structure . . . . .	4
<b>2 Literature Review</b>	<b>5</b>
2.1 Identity Governance and Administration (IGA) . . . . .	5
2.2 Online Government Services . . . . .	6
2.3 Related Works . . . . .	7
<b>3 Proposed Work</b>	<b>12</b>
3.1 Security Policy . . . . .	12
3.2 Proposed Security Model . . . . .	12
3.2.1 Effective Location of the proposed model . . . . .	13
3.2.2 Security Controls . . . . .	14
3.2.2.1 Identity Lifecycle Management . . . . .	16
3.2.2.2 Single Sign On (SSO) . . . . .	16
3.2.2.3 Credential Management . . . . .	16
3.2.2.4 Multi-Factor Authentication (MFA) . . . . .	17
3.2.2.5 Role-based Access Control (RBAC) . . . . .	17
3.2.2.6 Entitlement Management . . . . .	20
3.2.2.7 Automated Provisioning and De-provisioning . . . . .	20
3.2.2.8 Access Review . . . . .	20
3.2.2.9 Event Logging . . . . .	21

3.2.2.10	Segregation of Duties (SoD) . . . . .	21
3.2.2.11	Hierarchy of Authority . . . . .	21
3.2.2.12	Reporting and Analytics . . . . .	22
<b>4</b>	<b>Methodology</b>	<b>23</b>
<b>5</b>	<b>Implementation</b>	<b>24</b>
<b>6</b>	<b>Result and Analysis</b>	<b>34</b>
<b>7</b>	<b>Conclusion</b>	<b>40</b>
	<b>Bibliography</b>	<b>43</b>



# List of Figures

3.1	Proposed Security Model. . . . .	13
3.2	Proposed Model's location in the environment. . . . .	14
3.3	Security Controls. . . . .	15
3.4	Activity Diagram of Data Modification Officials. . . . .	19
5.1	Automated Provisioning Pseudocode. . . . .	24
5.2	Automated Deprovisioning Pseudocode. . . . .	25
5.3	Frontend view of Automated Provisioning & Deprovisioning. . . . .	25
5.4	Entitlement Assignment Pseudocode. . . . .	26
5.5	Entitlement Removal Pseudocode. . . . .	26
5.6	Role Assignment Pseudocode. . . . .	27
5.7	Role Removal Pseudocode. . . . .	27
5.8	Frontend view of Role based Access Control. . . . .	28
5.9	Login Management Pseudocode. . . . .	28
5.10	Login Page. . . . .	29
5.11	OTP Validation. . . . .	29
5.12	Email Change Pseudocode. . . . .	30
5.13	Password Change Pseudocode. . . . .	30
5.14	Frontend view of Credential Management. . . . .	31
5.15	Login Logs. . . . .	31
5.16	Action Logs. . . . .	31
5.17	Frontend view of Access review. . . . .	32
5.18	Figure: Frontend view of NID Modification (Demo). . . . .	32
5.19	Frontend view of NID Modification Validation (Demo). . . . .	33
6.1	Testing Result of the modules. . . . .	34

# List of Tables

6.1	Multi Factor Authentication . . . . .	35
6.2	Credential Management . . . . .	36
6.3	Role-Based Access Control . . . . .	37
6.4	Entitlement Management . . . . .	38
6.5	Access Review . . . . .	39
6.6	Event Logging . . . . .	39

# Nomenclature

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

*EC* Election Commission

*IGA* Identity Governance and Administration

*MFA* Multi-Factor Authentication

*NID* National Identity

*RBAC* Role Based Access Control

*SoD* Segregation of Duties

*SSO* Single Sign On

# Chapter 1

## Introduction

The Identity Governance and Administration (IGA) initiative allows clients and applications to securely exchange personal data. Fundamentally, Identity Governance and Administration (IGA) ensures secured e-service transactions over the internet maintaining data confidentiality and integrity. Applications and resources are protected and managed by it. In this prime time of the internet, successful implementation of e-services offered by the government is the sign of a digitally prospering/prosperous country. The successful deployment of e-government services is helpful for secured and fast transactions, reducing corruption, and boosting the economy eventually. As the application of e-government services is increasing more and more, this growth is posing a number of security and privacy concerns for customers i.e. citizens and businesses. One of these core e-government services in Bangladesh is online NID services, on which almost all other services depend. But, as stated earlier, these services are not protected as much as they should be. By using the knowledge of Identity Governance and Administration (IGA), it is surprisingly easier to protect these sensitive e-services infrastructures. The already existing NID system itself is a very vulnerable system and there have been a couple of incidents of Identity forgery using the existing system. With a little help from IGA practices, these illegal activities can practically be stopped. While working with the most important data collection of the entire country, it does not have to be explained how important and critical the security component of the NID system is. To keep on having the citizen's trust, strict security measures should be taken in such cases, but the incidents have not been seen to get the attention they deserve. The unauthorized and illegal activities happening within the system will not be eradicated unless proper steps are taken by the election commission itself. Through our in-depth research, we will dive into the pool of information regarding National identity services, its weaknesses and going forward we will try out different schemes and techniques as to how we can prevent such forgery incidents from ever happening in the future.

## 1.1 Research Problem

With the rapidly growing popularity and familiarity of all kinds of computer network technologies, online services have become very common around the world today. Real-time data sharing of government information and providing electronic government services has been available in a lot of developed countries for a long time now. According to the United Nations E-government Service 2020, approximately 22 percent of the world's countries use digital government services. Especially with the COVID-19 pandemic and lockdowns, it has pushed many countries to pursue digital government services. Likewise, Bangladesh, too, is advancing towards providing its citizens with eGovernment services. The Bangladesh government, according to the "e-Government Masterplan for Digital Bangladesh," is proactively working for digital penetration of all government portals by 2023 [18].

With this advancement, the risk of online exposure of valuable data belonging to the government and the citizens increases. According to Cisco, distributed denial-of-service (DDoS) attacks will increase to 15.4 million by 2023, more than doubling the 7.9 million recorded in 2018. E-government service does not only depend on the government; it depends largely on the people's readiness and trust to adapt to the online portals. Bangladesh is a developing country and has its limitations in accessing resources and information because of having less information about existing infrastructure. The country intends to develop economically with the help of the ICT industry. Bangladesh plans to employ information and communication technology (ICT) as a catalyst for socioeconomic development [1]. There have already been multiple attacks on the Bangladesh service, amongst which the Bangladesh Bank robbery incident was the most major, amongst several other ones. Although Bangladesh is now more sincerely working towards online security. The ICT department has taken on a huge project to work towards securing online services. The government now allocates more of the budget towards securing platforms more sincerely [1].

While discussing cyber security in Bangladesh and fully digitalising major government services online, besides the concern about the lack of resources, the next concern that comes to mind is pirated software. 90 percent of Bangladesh's software used is pirated [3]. Securing information is rather difficult, with most of the maximum population using pirated versions. Pirated software already comes with malware, exposing valuable information to cyber criminals. This may lead to information tampering where the attackers may change, delete, or insert data using technical methods and send it to the destination with the sole goal of damaging data integrity. Information stealing and information faking are the more palpable reasons for the attacks on the e-service system to commit national crime. Many of the software programs are not up-to-date and have poor maintenance in many government offices. Up-to-date software provides regular scanning and protection against malware on computers and repairs security gaps. According to a report by Kaspersky Lab, ransomware attacks on computers in Bangladesh have increased from 4-5 percent to 8.11 percent [21]. Besides, most officials in the country are not cyber-trained or aware of cyber crimes, further increasing the risk of exposure to hacking through phishing or giving unauthorized access to people.

It has been observed from the pre-existing models and online government service websites that a National Identity (NID) Card is the core requirement to use any of the services online. With the simple entry of a NID number, a bunch of information is available to a user. While this makes it easy for genuine users to access the system and retain information, it also makes the system prone to data theft and forgery. There have been many NID forgery cases reported recently. Due to the lack of identity governance, many field-level officers shared website passwords with data entry officers, which gave cyber criminals scope to forge NID cards [10]. Another such case was reported by the police where fake NIDs were being made for the purpose of taking bank loans [12]. This exposes the financial departments of the country to fraud and misleading data. Another such case was reported where people were able to manage the necessary documents for creating fake NIDs, including birth certificates, citizenship certificates, academic certificates, and other papers, through forgery, to register as voters as well as get the NIDs. [11]. Several other such cases have been reported over the years. Such cases are increasing with the country's exposure to technology and also with the limitation of resources and knowledge to prevent such issues. Such crimes exist due to the lack, or rather absence, of access control on websites. Bangladesh is a developing country with a dense population. It is going to take a long time, perhaps decades, to train or make people aware of cyber security.

National Identity Forgery has been going on for a really long period of time, very little attention is given to this unethical practice. Bangladesh being a technologically advancing country should handle this mal-practices as soon and strictly as possible. Identity Governance can contribute majorly to solving major parts of the problem, and it indeed will be a change which can be adapted in a shorter time period.

## 1.2 Research Objectives

The primary goal of this research is to develop an improved security model with advanced security controls for the National Identity eServices provided by the Govt. of Bangladesh, which will be based on Identity Governance and Administration (IGA).

The objectives of this research are:

- To get a better understanding of Identity Governance and Administration (IGA)
- To develop a Plug-and-Play (PnP) security model based on IGA
- To provide better security to Public's Sensitive Data
- To develop a model that will tackle National Identity Forgery more efficiently
- To develop a model that will prevent Fake NID generation
- To evaluate our proposed security model

## 1.3 Thesis Structure

This study is divided into a number of sections, each of which discusses the authors' methods of eventually arriving at their conclusion.

Chapter 1 - Introduction, research problem and research objectives have been discussed. This established the major topics for the authors to research and assisted the authors in working on those specific challenges.

Chapter 2 - Literature review, Identity Governance and Administration (IGA), On-line Government Services and related works provided reliable knowledge of IGA, eGovernment and a summary of all the research articles and journals through comparison and evaluation of similar research works in these fields.

Chapter 3 - Proposed work, Security Policy and Proposed security model describes in detail what security policy the model will follow, what the proposed model consists of, where it's effective location will be and finally how different security controls inside the model works fundamentally and the reasons behind using these controls in the model.

Chapter 4 - Methodology briefly discusses the different methods or techniques the authors followed to conduct their research till the end.

Chapter 5 - Implementation covers the design and the frameworks, the authors used, to implement their proposed work and all the pseudo codes of the security controls implemented and briefly explains the whole process.

Finally, Result & Analysis and Conclusion, in Chapter 6 and 7, provided outcomes of all the security controls implemented in the model and how the testing rubrics were used to evaluate them. The authors concluded with the limitations they faced in their work and their future plan to extend the model.

# Chapter 2

## Literature Review

The Internet as we know it is fast evolving as a result of the development of smart gadgets that can connect with humans and with each other over the Internet. With that, came the opportunity for the people's government to adopt this technology to provide services through the internet. This adoption has both the good part and the bad part. Quite a lot of authors wrote about everything there is to know and there is to adopt.

### 2.1 Identity Governance and Administration (IGA)

IGA stands for Identity Governance and Administration, which is also known as Identity Security. IGA is "both a policy framework and a set of security solutions that enable enterprises to more effectively minimize identity-related access threats within their business," according to Core Security. It enables an organization to monitor and guarantee that people's identities and security rights are properly handled, secure, and recorded, according to [20]. The benefits of using IGA include Password Management and Single Sign On tools, automated workflow, access request management, entitlement management, data logging and analysis [15]. IGA has become an important component for many companies for security purposes. About 80 percent of US companies with 1,000 employees or more make use of IGA systems.

This study [2] presents an Authorization-Function-Based Role-based Access Control (FB-RBAC) architecture for Enterprise Systems and Web Services that includes authorization-function-based access control as well as constraint-based fine-grained access control. This paradigm provides enterprise-level access control for systems where individual security systems are employed to safeguard one or more categories of resources. These security systems make authorization decisions depending on whether or not a subject is authorized to access a specific file or resource in a specific access mode. When systems access specific objects, such as database items, permission decisions are made in this manner.

This research [4] established a purpose-based access control approach based on a usage control model to improve security in the private data management of an E-healthcare system. Usage control gives you more control over how digital items are used. The model can also be used in a dynamic environment because the usage control model contains pre-Authorizations, ongoing-Authorizations, pre-Obligations,



ongoing-Obligations, pre-Requirements, and ongoing-Conditions, and a user must meet all of these conditions in order to be authorized. After meeting these requirements, users will be able to access purpose-specific information with their keys.

## 2.2 Online Government Services

Online government services, or E-government, are the use of modern communication tools, such as the Internet and SmartPhones, to provide public services to inhabitants and other people in a country or region (electronic government). E-government creates new opportunities for citizens to have more direct and convenient access to government, as well as for the government to directly give services to citizens.

In this paper [22], They have some insights for creating a successful e-government after analyzing the e-Government index between Arab countries and the top ten countries in e-Government. An effective e-government has three basic perspectives: the citizen perspective, the business perspective, and the governmental perspective. Moreover, for a successful e-government, Every project necessitates five types of skills: analytical abilities, information management abilities, technical abilities, communication and presentation abilities, and project management abilities. Furthermore, in order to develop a successful e-government, an integrated government service network that can reach citizens in both the physical and virtual worlds must be developed. But there are some challenges while implementing successful e-Government services that need to be considered, including: Infrastructure development, laws and public policies, the digital divide, e-literacy, and, most significantly, privacy, security, and transparency, among other things.

In this paper [9], they've introduced some secured e-government models that are being practiced successfully in different countries. In Dubai, they use a five-layered security architecture that includes a policy layer, a competency layer, a technology layer, an operational and management layer, and a decision layer. Each layer is composed of sub-layers and addresses different threats to e-services. In Egypt, they've proposed a hybrid cloud computing model consisting of three computing clouds: inter-cloud computing (private cloud), intra-cloud computing (public cloud) and extra-cloud computing (community cloud).

Furthermore, they discussed a E-government security model based on Service-Oriented Architecture and a Role-Based Access Control Model for developing secure e-government services in paper [9]. And lastly, they've proposed a security system based on the Information security model for e-government that adopts layers in its architecture that are more logical and thorough because they cover all the threats that e-governments face in each country. This system is modularized and is divided into initialization modules for managing original data, management modules for managing content that has an impact on the overall system, such as users, privileges, and a set of policies in the system, and various modules for completing the overall function of the system using the data that has been initialized and the transmission media.

## 2.3 Related Works

This section intends to conduct a critical evaluation of previous significant publications in the subject of eGovernment, Govt. electronic services, eServices Security, Security Techniques, eService Quality in the context of IGA. We analyze the different researches done on the topics and provide critical evaluation of these works in relation to the research problem we are working on.

Identity Governance and Administration, in short, IGA, is one of most efficient security techniques used in modern eServices. Digital Identity or eID is the main pillar of the whole implementation of this technique. For the betterment of Govt. eServices security, IGA will be a key tool or technique to implement. Through our research we got quite a lot of related works done earlier on the concerning topic and we reviewed and analyzed some of them critically.

In this paper [16] by S.N. Deekue, he proposes a strategic framework for eGovernment security in the context of Nigeria. The research emphasizes the fact that a generalized framework for eGovernment might not be an ideal choice for different countries with diverse governments and differences in a lot of characteristics. With that being emphasized, it is also clear that security measures taken for a particular public eService might not work for another eService. The author also states different aspects, concepts, and significance of e-government and its security. The research briefly discusses the security threats and vulnerabilities of existing eGovernment services and further describes some strategies and tools that may be used to secure these services better. Relating to that, our research focuses on the particular eGovernment service of the Election Commission, which works with National Identities. As this service proactively works with the public's sensitive data, it is not necessary to point out that this service needs much more advanced security than other eServices.

The research work [7] addresses the claim that secure identification tools are required for growing use of eServices and increase the validity of the government's eServices and describes the implementation process, analyzes security related to the use of the eService platform in their context. One of the main concerns described there is safe passage into the public eServices, which deal with citizen's sensitive information. According to the research [8], a safe passage into eGovernmental services is critical for security and trust in the eGovernmental services. Relating to this research, we also emphasize on the security of the public's sensitive information and focus on the controlled access to sensitive data. This research highlights the range of thoughts regarding secure log-in, system security aspects and management of sensitive data. If the citizens are to use and trust the eGovernment services, a security model with a great access management tool is a must have.

In this study done on e-government security risk management in China [24], the writers talked about the angles of risks e-government was facing in China when the country was new to the e-government system around 2008. Information interception, information tampering, service denial, system resource stealing, and information faking were among the highlighted security concerns, which might result in massive

vulnerabilities and loss for the government. The writers discussed the procedures of risk management. According to them, risk identification is the first stage in risk management in order to successfully change the security risks of e-government. The purpose of risk identification, they stated, is to identify warnings in the existing network in data or data interchange. Through risk identification, the potential vulnerabilities can be identified and be worked towards attack analysis and to control, prevent, and solve cyber attacks as much as possible. Risk Analysis is the next step of risk analysis. As discussed in the paper, by the analysis of risks through various qualitative or quantitative methods. Vulnerabilities on the listed warnings can be detected through spot investigations, people investigations, network scanning, penetration testing, related document analysis, or other open information sources. By the end of their research, the authors had devised risk management countermeasures. They suggested the use of a defense-in-depth strategy. This method includes multilevel security as well as security at deeper layers of system architecture. With the implementation of multi-level protection, full-proof system security can be ensured where if one level gets subdued, the other levels can still secure e-government system resources. Each layer will supply a different method to avoid the attackers from attacking all the different levels in the same manner. This paper gave us an insight into the state of another country when they were in the initial stages of introducing e-government services similar to where Bangladesh is at present.

In this research done on e-Government and Cyber Security [23], the writer talked about how exposing government e-service websites and systems to certain cyber exercises reveals the security status of the systems in the country. The exercises were performed to test the local government's ability to respond to viable cyber attacks. It tested how the system reacted to a less ideal environment. This exercise methodology allows the organization to test their policies and cyber attack procedures. The exercise targets disruption of local government operations using a combination of physical and cyber events. The conclusion the writer reached after running the exercise was concerning from the perspective of any country. It revealed various concerning weaknesses in the e-government system. Lack of preparedness, awareness, and understanding was observed across the board. Another major issue was government roles and responsibilities in the system. Maintaining the resources and operational state during an attack needs distributed resources and trained personnel. The exercise revealed gaps, vulnerabilities, access issues, and accountability issues in the system. We can learn from this article how regular maintenance and periodic testing of all e-government services can help bridge both technical and physical gaps in the system.

In this paper [19], there are three main concepts. These include: whether e-government service consumers are aware of how to obtain e-government services for their intended purposes; if the data on the platforms is accurate and reliable; and if the data on the platform is properly protected. Here, this study focuses on those users' perspectives who have used at least one of the e-government services of Ghana where the study considers some major security issues, including data accuracy, data reliability, hacking threats, data corruption, virus attack, modification of records, and data safety guards. So, for this study of user perceptions of data protection and integrity in Ghana, the first step they followed was research design

and sampling. The research population is all the end-users who have already used at least one of their e-government services, and the sampling has been done in a multi-stage process, e.g., region-based, city-based, and participant-based. The second step was research instruments and data collection procedures, where qualitative data was also extracted and analyzed. Furthermore, this study reveals that there are no service users who have no formal education at all, and to use e-services effectively, users need to have at least a basic education. Moreover, another finding was that the most used e-government services in Ghana are voter registration cards and election-related activities, health care services, and e-zwitch payment for financial transactions that work with a figure print identification and verification system. Besides, this study indicated that fewer users strongly disagreed or disagreed, and most of the users, over 70 percent, agreed that these services were available when they wanted to use them. Similarly, over 70 percent of users also agreed that information provided about how to use the services was clear to them, and a lower percentage disagreed with this. On the other hand, there are lots of errors in the record of the data on the systems, like spelling mistakes, wrong birth dates, wrong pictures with wrong names, etc. So, most of the users are not sure about the data and information accuracy on the e-government platforms. Now, in the case of data and information protection from unauthorized access, the systems are vulnerable to attack, and over 54 percent of the users agreed that e-government services are protected by firm hacking and unauthorized access, while the rest of the users disagreed or strongly disagreed with this issue. Finally, many users reported less reliable transactions, issues with information accuracy, unauthorized access, system unavailability when needed, and hacking risks. Based on all the weaknesses found in the study, they recommended Ghana take some steps: introduce more strict access control and create robust incident response teams to prevent unauthorized access; the equipment and software programs used need to be updated regularly and sourced from trusted parties; focus on public education to prevent about 80 percent of hacking problems; expand internet connection and make it more reliable and affordable to tackle the problem of service unavailability; to resolve difficulties regarding data verification and improve trust in e-governance; a national database with crosscheck and verification system can be introduced. Thus, Ghana can improve data integrity and data protection.

According to the paper [5], as Tanzania had the vision for developing the country's MDAs (government ministries, departments and agencies), this country has recognized ICT as a tool. Tanzanian e-Government strategy is also aimed at developing a security framework for their MDAs that is cost efficient and durable. So for that, a framework that is secured and conditions of the systems has been presented in the paper. But before that, they've considered several challenges which are categorized in 3 components as pillars – Governance, Operational and Technical. Governance challenges includes discrepancy on role of accessing sensitive data and information security where operational challenges includes inconsistency of implementing different action within different MDAs and technical challenges includes dissonance of storing sensitive data without proper security and management like database and operation systems were on different platform or no standard requirements for security were set. After considering these challenges, as a developing country, Tanzania considered a bottom-up approach instead of a top-down approach. And their framework is re-

ferred to by TOG which consists of 3 components as pillars as I've mentioned above. Here, technical component involves technical procedures for security requirements, operational component involves mainly plans, operational approach and governance component involves laws, national, international, regional standards and instructions, policies etc. These components match to the security objectives such as – confidentiality, integrity, availability, accountability and security requirements (access control, authentication, authorization, privacy, etc.) those are applicable to the e-government transactions. Furthermore, these components allow an MDA to allow flexibility in implementation and address information security comprehensively as well. This framework approach was dubbed as a plug and play or a top-down or a bottom-up approach where a PDAC (Plan, Do, Act, Check) cycle was followed for each activity. In this approach, it is possible to start to address information security by focusing on one pillar for any e-government transaction depending on the role of the department and availability of the resources and then move forwards a complete solution by mapping solutions from one component to another. Thus this TOG framework allows MDAs to include any of three solutions or practices for addressing secured transactions. After successful application of this framework, the evaluation of this framework indicates that this TOG describes almost all critical success factors and ISMS critical success factors proposed by ISO. Thus, a robust, cost effective and durable framework has been developed.

Researchers in [13] felt the importance of identity governance and management when the outbreak of the COVID-19 pandemic had increasingly led industries, educational institutions, and some other institutions to move to work online from traditional methods. This paper focused on the access control of privileged users in a system using the Active Directory service. The paper also proposes an integrated approach by including IAM (Identity Access Management) being an authentication tool and PAM (Privileged Access Management), which is able to enhance privacy and protection by reducing the data flow in transactions. The proposed framework provides 86 percent security, which is more stable compared to other existing access control security frameworks.

The need of having continuous protection with information security controls that travel with a system's data at both the network and physical levels is stated in this study [17]. This study presents a Role-centric Mandatory Access Control MAC (R-MAC) paradigm as a security intermediate between the service pleader and the service provider to offer authentication and authorization for Saudi Arabia's e-government web services. This concept combines XML security technology with a data classification strategy appropriate for e-government information, allowing unknown people to gain dynamic access to the system while maintaining persistent control over the information.

In this paper [14] by R. Hill, he highlights the necessity of identity governance and management. He quickly described how the leadership compass now evaluates more than 20 percent more IGA products than the previous year, indicating that the IGA market is expanding as a band that now offers a cloud IGA product that is cloud deployable with ready integration with popular cloud applications as well as standard on-premise applications.. This method is better suited to organizations that

have an MSc strategic emphasis on cloud migration and want to reap the benefits of cloud adoption. Identity lifecycle management is defined by terminology such as identity repository, password management, access request management, policy and workflow management, and role-based management. He then went on to talk about access governance, which encompasses identity analytics and artificial intelligence, access certification, and role governance. There was a role defined in the government, which is a role based on business function and logical grouping access. Controls that are important to detect, track, and move are referred to as soD control management. He also mentioned reporting and dashboarding, which is the process of converting important data into formats that are easily understood by business functions. Delivery models as well as essential competences had a significant influence.

In this paper [6] by Yazeed Alkhurayyif, he wrote about national ID cards. He began by discussing its history and then addressed the issue of national ID card privacy, stating that it may be hacked or that firms could profit from the information. He also stated that the government introduced smart ID with biometric systems that have many functions, but it is still debatable because implanted chips can record all data, which could lead to hacking. He then went on to explain the benefits of having a national ID card. Illegal labor and immigration, crime prevention and potential terrorist attacks, improvement of access to public services, and compiling data onto a single card are among them. He also mentioned several downsides, such as cost, concerns about privacy and the usage of identity cards. He also talked about security properties. which has a domain-specific unique access control mechanism. Identity, selective disclosure, verify-only mode, biometric templates, and availability are all factors to consider. He also examines the rate, which includes human mistakes, counterfeit identities, content falsification, and man-in-the-middle attacks. He then went over some possible possibilities. Small card chips, for example, were installed on each credit card by UK Biometrics Limited. He also claimed that this solved the hacking problem, which involves the sharing of personal information between parties. Finally, he stated that the effectiveness of national ID cards in improving national security is still debatable.

From the above discussion, it is observed that most of the researchers approve the necessity of IGA and its implementation in Government services.

# Chapter 3

## Proposed Work

The proposed security model we are working on, will be developed based on a strict security policy. It will be a plug and play model, meaning it can be easily plugged into the already developed system of national identity services. In accordance with the research we have done through-out this phase, we defined the security policy that will best work with our research problem. Our work will fully focus on developing the model that enforces our security policy.

### 3.1 Security Policy

If we were to classify our security policy in terms of major forms of information security policies, our policy will be classified as a Prudent Policy. What is meant by a prudent policy is that, the policy would be a high restriction policy where every resource or access to resource is blocked from the get-go. Necessary services needed for further work will be allowed to be installed by the administrator. Every activity gets logged for every user and gets maintained throughout the system. Our policy has the same kind of restriction and set of rules to control every sensitive activity securely. In our policy, any type of user joining the system will not directly get privileges right from the start. Rather, the system or administrators will manage roles and privileges to services and resources based on necessities. Moreover, The system will log anything and everything done within the system. Ensuring security to data and resources is the first priority in our security policy. Relating to our purpose in this research here, identifying forged national identities is not our policy's purpose, rather our policy will facilitate the whole process of preventing identities to be ever forged in the first place. Through our research we got the idea of how these identities are forged and these are mostly done mis-using the current vulnerable system. The proposed policy will enable our model to be developed easily and strictly focused on our research purpose.

### 3.2 Proposed Security Model

The purpose of our proposed security model is to secure the existing NID system and prevent NID Forgery using the security controls as described in the following

chapters. Figure 3.1 below, provides an interactional depiction of our proposed security model.

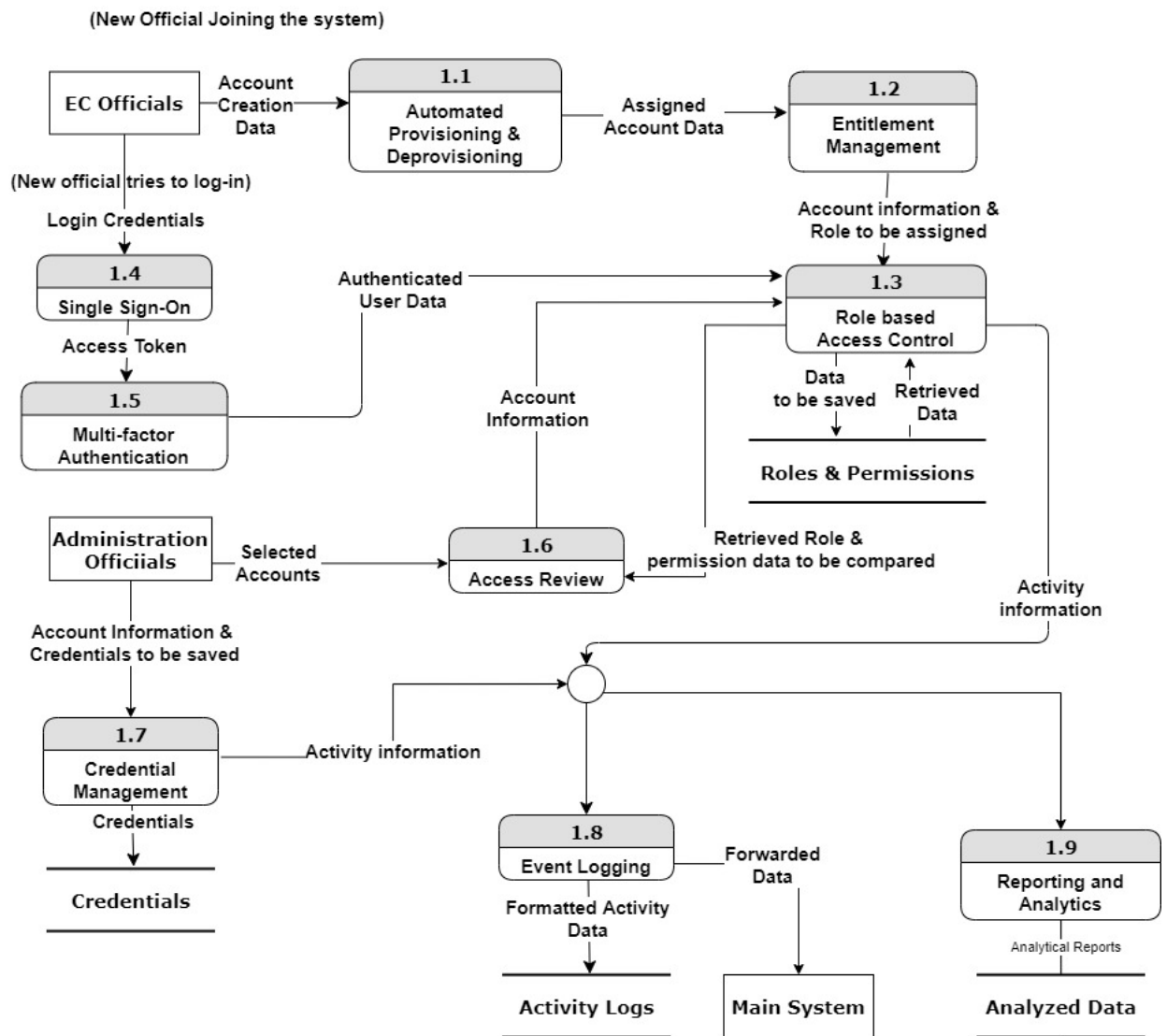


Figure 3.1: Proposed Security Model.

The proposed model which is designed defining the above mentioned security policy, has a set of security controls and defined roles & privileges for users as seen in the figure above. The following chapters will give brief ideas of what each of the security control and other aspects of the model.

### 3.2.1 Effective Location of the proposed model

As mentioned earlier in the research, we are designing our model to be a plug-and-play model. This makes it easier to integrate with the already existing system. In the figure below, we have shown the effective location of our proposed model in the existing system environment:



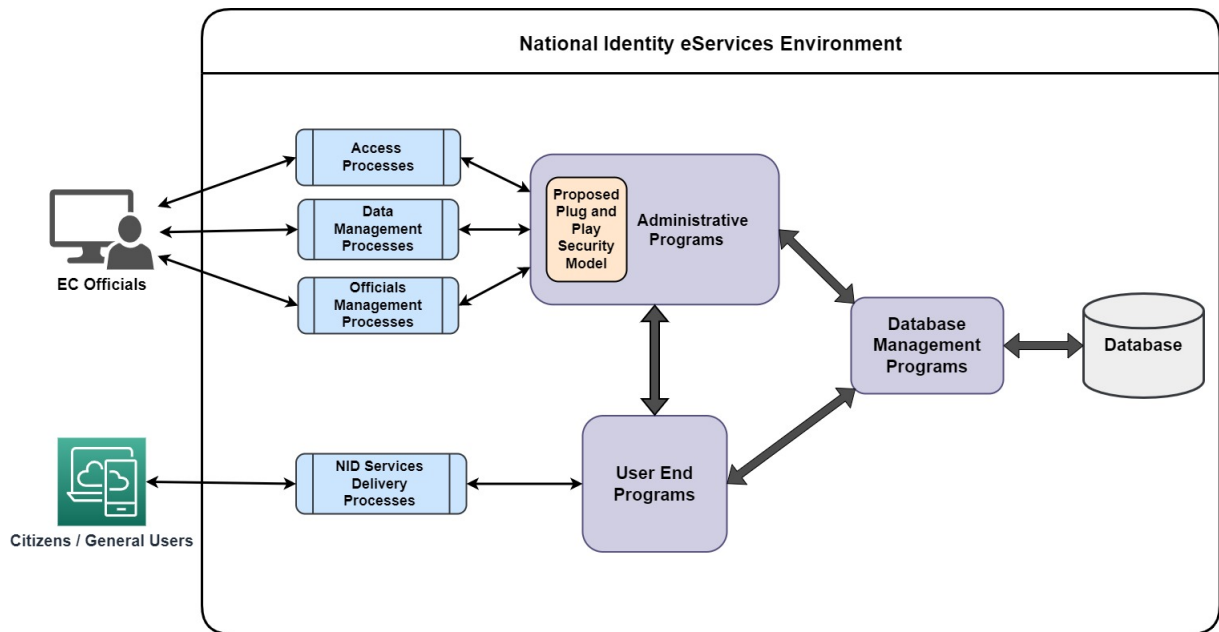


Figure 3.2: Proposed Model's location in the environment.

### 3.2.2 Security Controls

Security controls are any specific type of tools, techniques, software or any measures taken to counter or mitigate specific security risks in any system environment or property. In information security, these security controls are generally implemented to protect information, Intellectual property and Technologies.

#### Security Control Types:

Security Controls can generally be of 3 types.

1. **Physical Controls :**

These types of controls are solely used to protect physical systems or assets. These measures can be physical devices or entities or even a person as they protect a physical asset.

2. **Technical Controls :**

These controls are typically softwares or sometimes can be hardwares. As the name suggests, they usually protect technical assets. Examples of technical controls would be Intrusion Detection System, Access Control Lists etc.

3. **Administrative Controls :**

These types of controls are mainly guidelines, policies, procedures defined according to any organizers' security plans. These measures can be physical devices or entities or even a person as they protect a physical asset.

#### Security Control Functionalities:

Security Controls can also have 3 types of functionality:

1. **Preventive Controls :**

These types of controls are designed to prevent or stop risky activities in any system before occurring.

2. **Detective Controls :**

These types of controls are designed to specifically and technically detect risky activities or resources in any system when they get executed or in-progress.

3. **Corrective Controls :**

These types of controls are designed to repair the damages cost by any risky activity in any system after they have affected the system somehow.

Our security model consists of several security controls or security control modules which fall under the type of Technical and Administrative Controls with Preventive and detective functionality. These controls will be solely used in the model to enable strict security. These modules can be put into different sets according to their types based on Governance or Access management as seen in Figure-3.3.

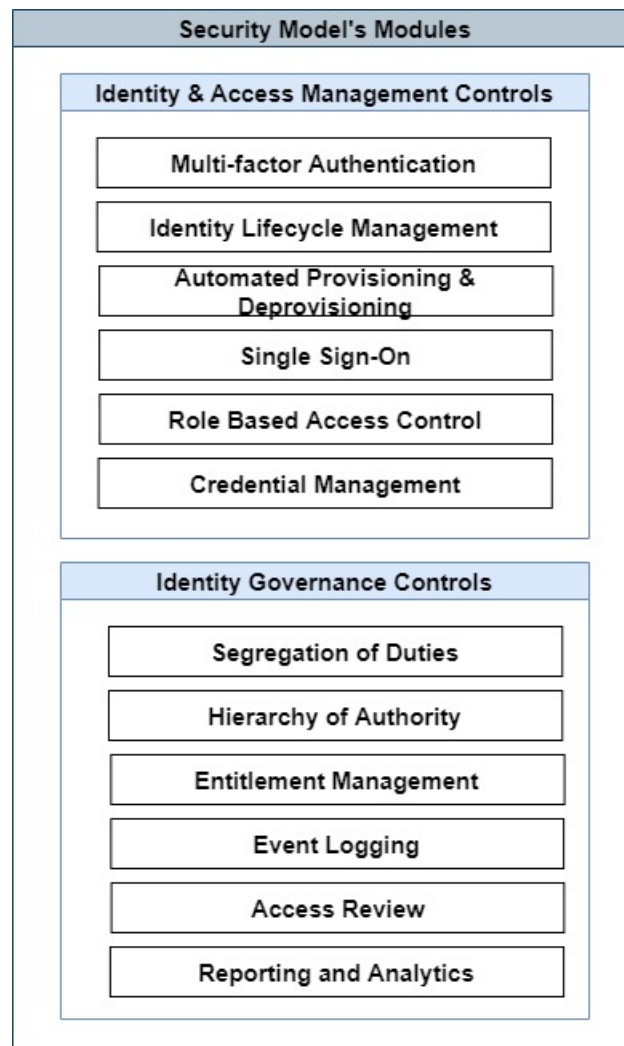


Figure 3.3: Security Controls.

### 3.2.2.1 Identity Lifecycle Management

Identity and Access Lifecycle is a term for the full life cycle of identity and access for a user on a given system. In our context, this system handles the entire process of someone getting in and out of the system. There are several stages of Identity and Access Lifecycle similar to any general lifecycle in the identity lifecycle management system.

**User Onboarding:** Whenever a user will enter into our system, s/he will need an account with digital identity. Once a user gets access to the system, we'll use automated user provisioning for providing privileges to these new users.

Provisioning will be done using RBAC. RBAC or Role Based Access Control is basically an identity management system which restricts or provides user access based on their role assigned by the organization. It basically defines what users can do or can't do according to their roles. By implementing Role Based Access Control we can restrict access to the sensitive and important data.

RBAC will use the security control called Entitlement Management that will basically assign permissions to the user according to the role.

**User access and system usage:** After successful account creation, a user will be able to log in to our system using login credentials into our Single Sign On (SSO) client. These login credentials are managed by the control called Credential Management. After successfully passing the Multi-factor authentication, a Single Sign On (SSO) session will be set up for that user and the user will get access to the system.

**User offboarding:** Whenever a user will leave our organization or a user account needs to be discontinued or deleted, all the access of that user will be removed using Automated Deprovisioning. Deprovisioning simply revokes permission and unauthorized user identities to the system. It is a very important security control to ensure that system access integrity is kept. It prevents data exposure to unauthorized personnel and removes expired accounts.

And thus, with user offboarding, the Identity and Access lifecycle of a user will conclude in our system.

### 3.2.2.2 Single Sign On (SSO)

Single Sign On (SSO) is one of the most important security controls in our model. SSO is an authentication process to authenticate users in multiple applications which are under one system by using only one set of credentials. It is, in simple words, a unified and centralized login system. In our model, whenever a user logs into the system using an SSO client, the SSO server will create a session for that user and s/he will be able to access all the respective applications with that session.

### 3.2.2.3 Credential Management

Credential Management refers to tools of identity verification of a user in a system. It is a form of software which is used for issuing and managing credentials of users in the system as part of public key infrastructure. The user may be part

of an authentication process that helps confirm their identity in relation to a network address or system ID. Throughout a user's lifecycle in the system, the user will face changes and adjustments to their system credentials and secure resource access.

In our system, credential management plays a key role. From lost or stolen passwords of any official to when an official is no longer part of the organization and requires updated access to the system, credential management is the security control responsible for handling such cases. To elaborate, if an account gets stolen, the account immediately needs to be retracted to avoid access abuse. This is where efficient credential management comes into play. Proper credential management will allow you to instantly block the account and/or change credentials of the account and prevent unauthorized activity. The same applies for situations when an official is no longer part of the organization, his/her account needs to be deprovisioned from all access rights. Credential misuse brings huge vulnerabilities to the system and thus it is essential to have an efficient credential management that covers every stage of a user's lifecycle from resetting and retraction to replacement and access updates. To prevent any unwanted activity all events are logged into the event log to detect suspicious activity if any.

#### **3.2.2.4 Multi-Factor Authentication (MFA)**

Multi-Factor Authentication or MFA is an authentication mechanism that requires a user to go through multiple authentication/verification stages in order to get access to a system such as an application, an online account, or a virtual private network. A strong identity and access management (IAM) based security policy must include multi-factor authentication. Multi-factor authentication needs more extra verification criteria in addition to a username and password, that reduces the chances of a successful cyber attack.

We will use this in our model to verify user legitimacy. For all levels of officials or users, we will use this Multifactor authentication. The model may use Security tokens which are small hardware devices that hold a user's personal data and are used to electronically verify that person's identification. A smart identity card or an embedded electronic chip in a device such as a USB drive, or a wireless tag might all be used as the device. The purpose of multi-factor authentication (MFA) is to construct a layered protection that makes it more difficult for an unauthorized person to get access to a system. Even if one element is compromised, any attacker still has to overcome one or more barriers before gaining full access to the targeted system. In our model, If anyone gets a password from an official, he or she will not be able to log in easily due to use of MFA.

#### **3.2.2.5 Role-based Access Control (RBAC)**

Role Based Access Control (RBAC) refers to the mechanism of restricting system access to users based on that user's roles and permissions within the organization or rather the system. RBAC ensures that employees have access to the resources within the system, only the ones specifically according to their jobs or roles in the

workplace. This maintains a system and information hierarchy within the organization and helps prevent system abuse.

For the above reasons, RBAC is a crucial and significant method for our model. The role based access control model is based on several factors such as authorisation, responsibility and job competency. We have designated the roles of the employees of our system into groups such as, higher officials, admin level officers, data entry and modification officers etc. Each group of users can only perform certain tasks and have to go through a certain verification procedure for entering and/or using the system. Access to the system resources are limited to specific user groups such as view, create or modify. For example, the Data Entry & Modification Officers can only enter new data to the system and modify existing data of the system only. That too, the data modifications that are done by these officers are verified by the Verification Officers to ensure no misuse of the system.

### **The roles defined in our model :**

- Top Level / Higher officials: The most trusted/ top authorized group of officials in the system who will have access to the top secret level information in the system hierarchy. These officials will have the ability to handle the permission granting tasks but might rarely use that.

#### **Permissions:**

- Can view top secret level data or information
  - Can set /change permissions of lower level users in the system
  - Can view activity logs.
  - Can manage credentials
- Administrator level officials: Will be responsible for administering the whole system.

#### **Permissions:**

- Can set /change permissions of lower level users in the system
  - Can allow a system manager or security officer to add,change, or delete interface options that can control the operation of the interface
  - Can manage credentials
- Verification officials: These officials are exclusive and will be responsible for verifying data modifying activities that are being initiated in the system by data modification officials. Everytime a data entry official makes any request to change NID information, the modification request is sent to a 'Modification request' log from where the Verification official reviews and accepts the modification which is only then updated to the main NID database. This task dependency is a mechanism called 'Segregation of duties' which will be elaborately explained later on.

### Permissions:

- Can view the the data modification requests
- Can verify, cross-check data and accept data modification requests.

The data entry officials' tasks are very sensitive and it will be guarded with extra security measures to ensure least chances of illegal activity. Data entry officials will not have full access to the system. Everytime a data entry official wants to access the system, their device will be provided with a token using which the data entry officials can request data modification or enter new data. The token validity will be constricted to a specific number of modifications per session and might have an expiry period of several specific hours.

The diagram below (Figure-3.4) illustrates the activity flow of a data entry official:

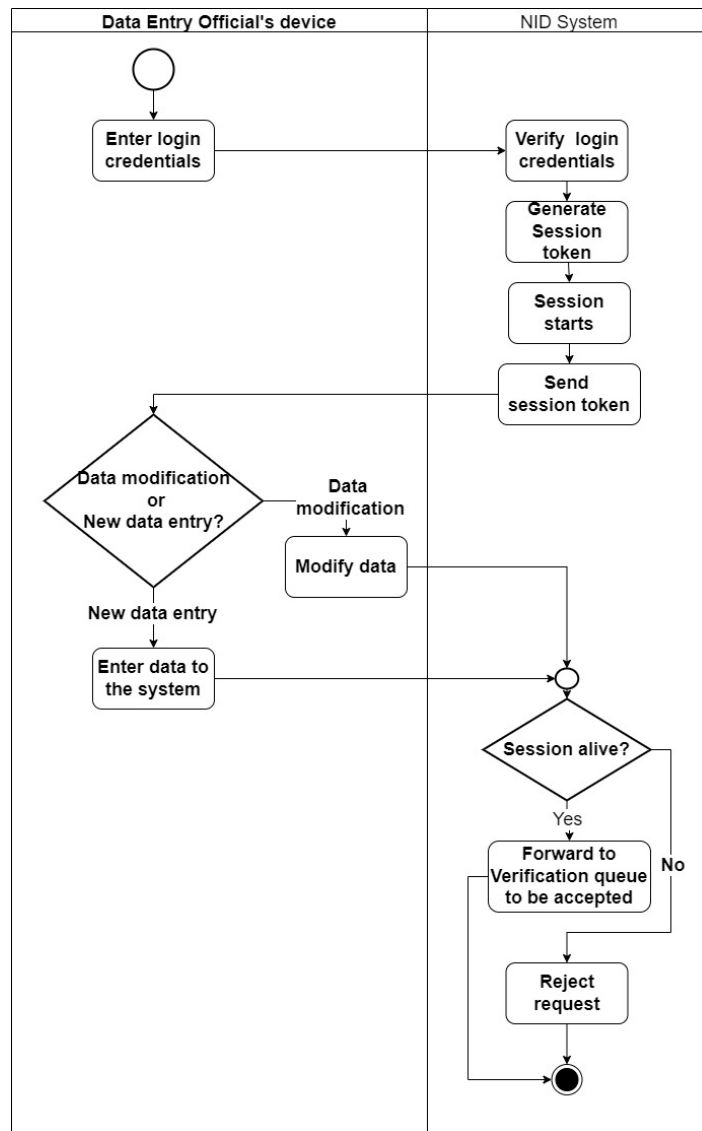


Figure 3.4: Activity Diagram of Data Modification Officials.

### **3.2.2.6 Entitlement Management**

Entitlement Management refers to the method of managing the process of giving/assigning roles to any user and with that role the corresponding permissions. Entitlement management is an Identity Governance mechanism which handles this important role of deciding which role and permission to give to which user. It is a part of the whole Role-based Access Control technique. Entitlement Management in our model is implemented for the purpose of handling roles, access and permissions.

### **3.2.2.7 Automated Provisioning and De-provisioning**

Automated Provisioning or Automated Access Provisioning refers to the concept of granting access permission of a user to the associate software automatically whenever a new user is assigned a role. Users can have access to the specific app they are assigned to or specific resources according to a role associated with that user that ensures the security of a company.

In our model, Automated Provisioning will be used when any official is registered and gets assigned a role in our system. Using this method, s/he will have access permissions automatically in accordance to that role. For example, If an official is classified as a modification official, then the official will have the access to view NID informations and modify them if needed (Time-limited). Similarly, in another case, being classified as an Administrator level official, the user will be able to set /change permissions of lower-level users in the system.

On the other hand, Deprovisioning means terminating a user's access right from the whole system. In our model, this process will be fully automated. We need this when an authority resigns or leaves the organization, then all of the access rights of that account will be removed automatically.

### **3.2.2.8 Access Review**

Access review refers to a periodic review of access rights of all users in any system. This security control allows us to cross-check user privileges so they can be changed or revoked when required. Access reviews can help deal with a lot of vulnerability within the system. In our model, the access review process will consist of the reassessment of official roles, access rights, privileges and credentials provided to the officers. During the review, special attention will be given to the officials who have recently been promoted, officials who have taken on new responsibilities and officials who have worked with the organization for a long time. It may occur that a long time employee was given temporary responsibility and so access rights were provided. However, the officer was not deprovisioned from those temporary access rights. This opens the system upto security breaches and thus needs to be periodically re-assessed. Access review is an essential control in our model to prevent privilege creep, excessive privileges, access abuse, costly employee errors and insider threats.

### **3.2.2.9 Event Logging**

Event logging is the logging mechanism where it will log every activity and provides a single channel for programs to capture critical software and hardware milestones. We can see who is logging in and who is engaging in which activity on the system. Using event logging, we can also see who is initiating which task. It might also log the user's log in and log out timings. This technique assists us in easily detecting any unusual activity on a system.

Event Logging is used in our model to keep track of every activity. Any unethical or fraudulent attempt or unauthorized activity can be easily traced with the help of logging. Then the authorities can take the necessary action against that faster than the current system.

### **3.2.2.10 Segregation of Duties (SoD)**

Segregation of duties in information security refers to an internal security control that divides a whole process into different tasks and then is assigned to different levels of authority. The duties and associated risks of each role of every authority should be specifically defined. In our model, duties will be segregated into different authorities based on their hierarchical position after setting the hierarchy of authority.

As the processes are divided and assigned to different authorities, it eliminates the over amount of control over a single process of a single authority which can prevent the risk of security threats to a system. As the purpose of our system is to eliminate the forgery done by the field level officials because they often misuse the power of having unauthorized access to Ec's main server, that's why segregation of duties will be much more efficient to restrict them from doing this. To explain further, If there is any need to modify any NID information, Data entry officials will modify the information but cannot update the modified information directly into the NID's main server. After each modification by the data entry officials, the modification request will be sent to verification officials who are the next higher level of authority and after verification, if the information is found authentic, only then it will be updated into the NID's main database.

In this same situation, verification officials will only be able to view and verify the information entered by the data entry officials. After verification, they will either accept or decline the modification request based on the authenticity of that data, but cannot modify the data themselves. That is how this crucial task is divided into two processes which prevents misuse of the system.

### **3.2.2.11 Hierarchy of Authority**

Hierarchy of authority is a technical control which is essentially a process of ranking the authorities into different levels, one above another from top to bottom, with some access rights and a set of roles based on their position. Top officials fall under the top level in the hierarchical position and will have the highest level of decision-making power. On the other hand, the bottom level of authorities will have the least level of decision-making power.



As our system requires specificity about every classified user's role, that's why the hierarchy of authority is needed to clearly define what each authority is supposed to do or be doing. Moreover, each authority has to have accountability for their job to the next level of authority. A hierarchy of authority will strictly ensure this.

According to the recent NID forgery incidents that are happening in Bangladesh, the culprits are mostly the field level authorities of the NID server who are mainly the data entry officials. They have direct access to EC's main server. After modifying any NID information, that information is being updated directly into EC's main database. As a result, they often misuse this power which means there is no boundary of access rights and roles between authorities based on their hierarchical position. That is why our model will use Hierarchy of authority's concept to provide extra restrictions to these field-level officers so that the security of NID services is not compromised at any cost.

### **3.2.2.12 Reporting and Analytics**

Reporting and analytics can assist commercial organizations in improving and production in a variety of ways. But, This is also a detective control which can assist our model in figuring out what is happening throughout the system. Reporting explains in short and sorted format that's easy to understand by the associated authorities, whereas analytics allows us to go deeper into the data and gives a priceless insight of the whole system. Both of these are critical for an organization's ability to make well-thought choices by showing facts in an easily understandable format. Activity insights and statistical information is included in these analyzed reports.

In our model, we will use reporting so that we can find every information about any official and their activity, this will help us to easily locate and identify the culprit. Reporting takes help from event logging in this process.

All the security controls defined above will enable us to successfully reach our main goal which is preventing Identity Forgery misusing the system and strengthening the security in the process.

# Chapter 4

## Methodology

In the governmental system, the security model we're putting out will operate in a very delicate area. This is the primary reason we had to choose our study methodologies extremely carefully. There isn't much information accessible to the public regarding the NID system because it provides a sensitive government service. Our study was conducted using qualitative techniques. For our investigation, we had to carefully and critically use all of the information that was already accessible online about the NID services. The aforementioned system's problems and errors had all been around for a considerable amount of time and had only become worse with time. We learned a lot about the systemic falsification or forgery incidents from reliable sources and news portals because it was widely covered in the press. As we identified and recorded every system flaw that led to the forgeries, we dug deeply into each one to determine its most likely root causes. Further study revealed several reasons and solutions, and eventually we came to the conclusion that the "Identity Governance and Administration" modules would be a perfect way to address the forging issue. After that, we tried with various modules and techniques to address each fault we discovered. We ultimately chose to adopt the current modules included in our security model after careful deliberation and testing, evaluated the outcomes, and obtained the desired outcome.

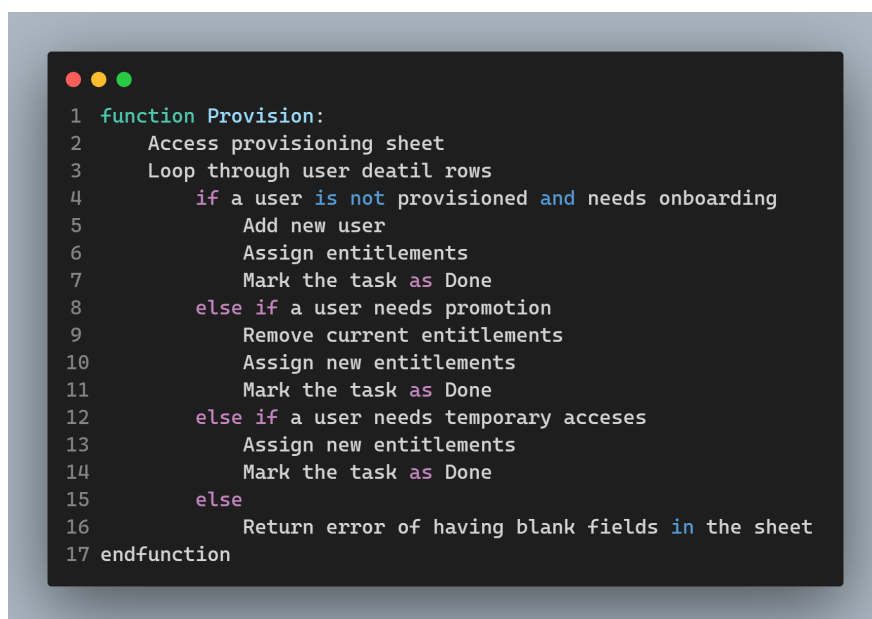
# Chapter 5

## Implementation

To implement our security model, we followed a modular system design. Each security control in our model was designed as separate modules which can be put together in our designed pattern to complete the whole process of the system. We created all of these using NodeJS & ExpressJS as the backend. To make the whole process incredibly simple to understand and use, we utilized VueJS as the frontend to provide a very simple front view by encapsulating all the complexity in the backend. MongoDB met our demand for a document-based database to store various pieces of data in the system. Now, let's get an idea of how each security control works as a separate module or a unit.

### Automated Provisioning and Deprovisioning:

This module will get the necessary data to provision or deprovision users, from two Google-sheets, one for Provisioning and another for Deprovisioning. The pseudocode seen in the image below is how the actual module is handling provisioning of every user.



```
1 function Provision:
2   Access provisioning sheet
3   Loop through user detail rows
4     if a user is not provisioned and needs onboarding
5       Add new user
6       Assign entitlements
7       Mark the task as Done
8     else if a user needs promotion
9       Remove current entitlements
10      Assign new entitlements
11      Mark the task as Done
12     else if a user needs temporary access
13       Assign new entitlements
14       Mark the task as Done
15     else
16       Return error of having blank fields in the sheet
17 endfunction
```

Figure 5.1: Automated Provisioning Pseudocode.

The deprovision works almost the same way as the provision pseudocode but does the job of automatically offboarding a user from the system and update the google sheet. We can get an idea of how it works by watching the pseudocode given below:

```

1 function Deprovision:
2   Access deprovisioning sheet
3   Loop through user deatil rows
4     if a user is not deprovisioned
5       Remove that user
6       Mark the task as Done
7     else
8       Return error of being unable to deprovision
9 endfunction

```

Figure 5.2: Automated Deprovisioning Pseudocode.

The official responsible for initiating the processes of onboarding or offboarding will not have to understand the backend’s complexity. He/She will have the simple interface to operate as seen in the following image. He/She just needs to update the provisioning sheet with specified inputs and then initiate by clicking the ‘initiate provisioning’ button and the system will automatically process everything needed. The same goes for the deprovisioning part, the instructions are clearly given righ! above the workspace too.

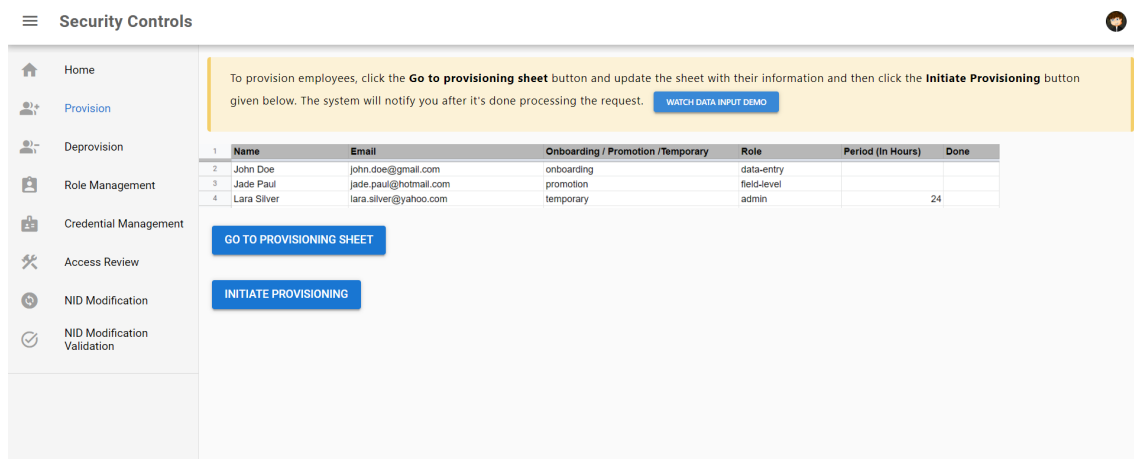


Figure 5.3: Frontend view of Automated Provisioning & Deprovisioning.

### Identity Lifecycle Management:

The ‘Automated provisioning & deprovisioning’ module is strictly managing the identity lifecycle in the system automatically.

## Entitlement Management:

This module is responsible for providing users with appropriate roles and that too, for a specified time period. Automated provisioning & deprovisioning invokes this module automatically to process all the entitlements. The image below shows the pseudocode of how an entitlement gets assigned to a user.

```
1 // Takes the user that should be assigned a particular entitlement,  
2 the entitlement reference  
3 and the active period of the assigned entitlement as input  
4  
5 function AssignEntitlement:  
6     assigns the entitlement as a role using Role based access control module  
7     if assignment is successful & entitlement active period is not provided  
8         schedule a cronjob to remove the entitlement after the given period  
9     else  
10        Return error of being unable to assign entitlement  
11 endfunction
```

Figure 5.4: Entitlement Assignment Pseudocode.

And, the following image shows the process of entitlement removal. Both takes help from another module named 'Role based access control' or in short RBAC, to handle the role management part.

```
1 // Takes the user to remove a particular entitlement  
2 and the entitlement reference as input  
3  
4 function RemoveEntitlement:  
5     removes the entitlement as a role using Role based access control module  
6     if removal is successful  
7         schedule a cronjob to remove the entitlement after the given period  
8     else  
9         Return error of being unable to remove entitlement  
10 endfunction
```

Figure 5.5: Entitlement Removal Pseudocode.

## Role Based Access Control (RBAC):

RBAC is doing the job of managing all the roles and role-related tasks in the system. Creating a permission, creating roles or even assigning or remove a role is handled by this module. The tasks of assigning or removing user roles will be automatically invoked by previously discussed modules and no official will have manual access to

them. In the following image, we get to see the pseudocode of assigning a role in the backend.

```
1 // Takes the user that should be assigned a particular role,  
2 and the role reference as input  
3  
4 function AssignRole:  
5     assigns the role to the user by updating in database  
6     if assignment is successful  
7         return true  
8     else  
9         Return error of being unable to assign role  
10 endfunction
```

Figure 5.6: Role Assignment Pseudocode.

The following pseudocode shows the process of removal of a role in the backend.

```
1 // Takes the user to remove a particular role,  
2 and the role reference as input  
3  
4 function RemoveRole:  
5     removes the role from the user by updating in database  
6     if removal is successful  
7         return true  
8     else  
9         Return error of being unable to remove role  
10 endfunction
```

Figure 5.7: Role Removal Pseudocode.

The official handling the these processes will see the interface below, to operate the tasks.

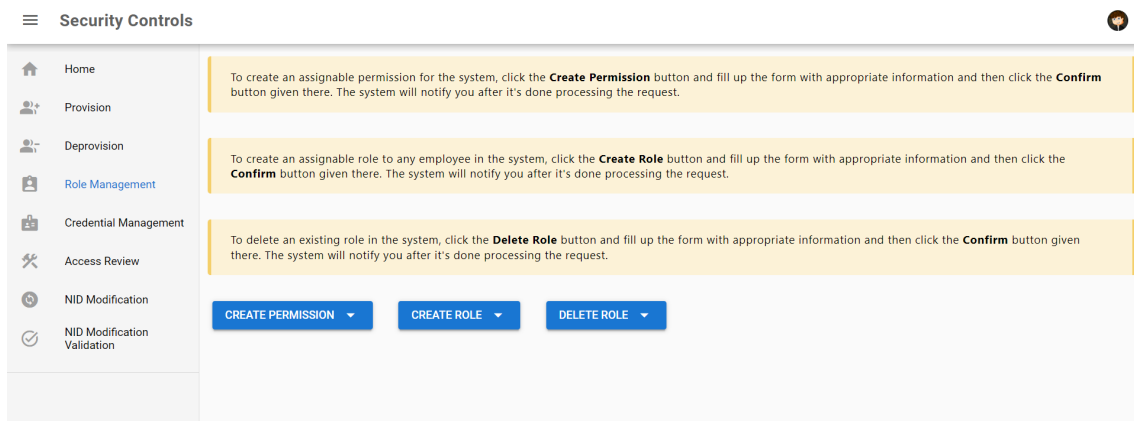


Figure 5.8: Frontend view of Role based Access Control.

### Hierarchy of Authority:

RBAC is designed in a way that will maintain the hierarchy of authority inside the system. This simply means that higher level officials will have higher level access and the hierarchy will be maintained as the roles given to each officials.

### Multi-Factor Authentication (MFA):

This module handles the proper authentication of a user entering the system. We are using two factor authentication in this case, primarily. The first factor would be Password input and the second one is OTP Validation sent to user's email. The following image shows how the process works.

```

1 // Takes the username/email
2 and the password as input
3
4 function Login:
5     retrieves the user from database
6     if user is not found
7         return error of User not being found
8     else
9         if given password == password from database
10            sends OTP to user's email
11            return 'OTP has been sent to user's email' message
12        else
13            return error of Incorrect Password
14 endfunction

```

Figure 5.9: Login Management Pseudocode.

The following images of the frontend shows the Login page and the OTP validation page triggering the module in the backend.

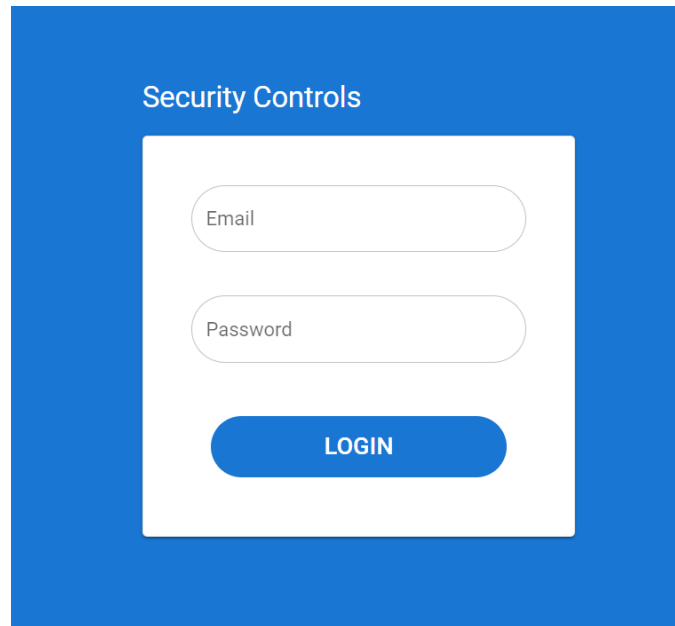


Figure 5.10: Login Page.

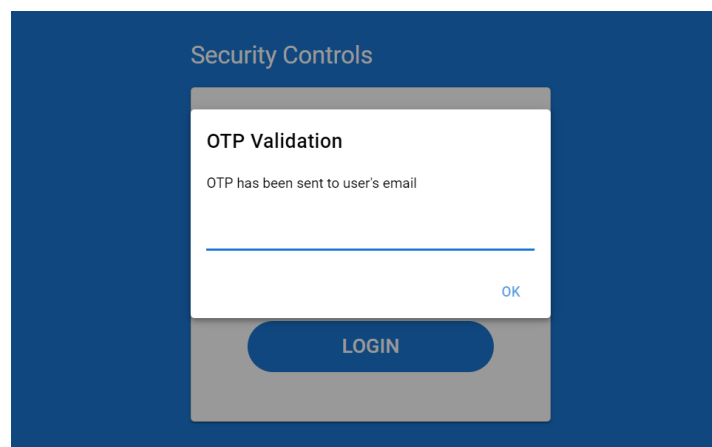


Figure 5.11: OTP Validation.

### **Single Sign On (SSO):**

This module handles the different infrastructural login inside the system where it will centralize the login to all the available apps. The users will not need to login each time when they use a different app in the system. However, we couldn't build the module because of lack of available information of the apps and other accesses provided inside the Election Commission organisation. With proper information and data of how the internal organisation works, it will not be that hard to implement Single-Sign-On in the system.

### **Credential Management:**

This module is responsible for changing any user's login credentials in the system. In case of, user's email change or compromised password, the module will help to automatically process the request, once initiated by the admin. The following pseu-



docodes will give a brief idea of how the backend works when the task of changing email or password is initiated.

```
1 // Takes the previous email
2 and the to-be-assigned email as input
3
4 function changeEmail:
5     retrieves the user from database
6     if user is not found
7         return error of User not being found
8     else
9         updates the user's email with the to-be-assigned email in the database
10 endfunction
```

Figure 5.12: Email Change Pseudocode.

```
1 // Takes the current email as input
2
3 function changePassword:
4     retrieves the user from database
5     if user is not found
6         return error of User not being found
7     else
8         generates a new password
9         updates the user's password with the newly generated password in the database
10        sends the new credentials to the user's email
11 endfunction
```

Figure 5.13: Password Change Pseudocode.

The admin will have an easy interface to initiate these tasks as seen in the following image:.

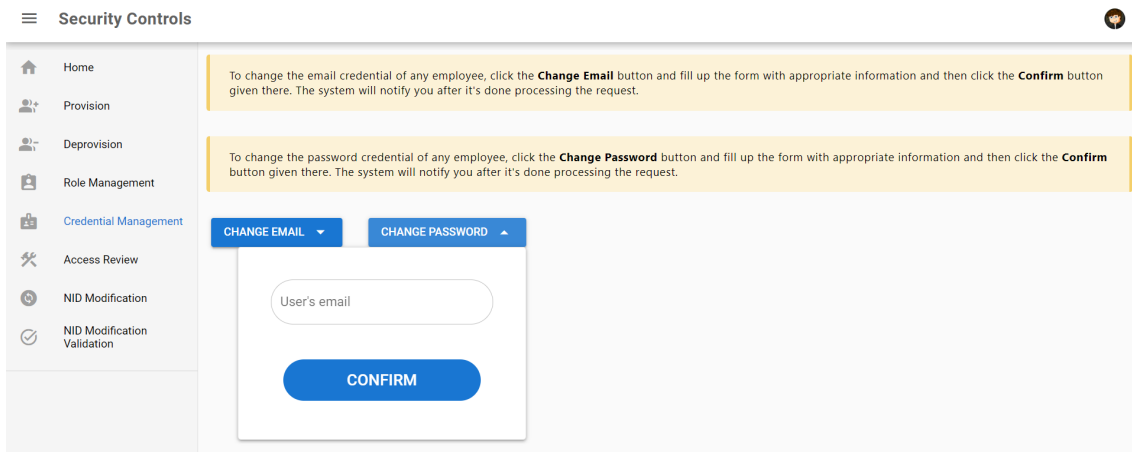


Figure 5.14: Frontend view of Credential Management.

### Event Logging:

This module logs every activity initiated in the system. The technique is very effective in detecting and finding culprits out faster than usual. It will log all the login and logout sessions in a dedicated log file. It will also log all the actions initiated by any officials in a separate log file.

The following images are showing the log files with the logged activities and also mentioned the initiator and the time they got initiated.

```
login.log M X
backend > login.log
1 User Login: Logged in as 'testuser1' at: 00:22:54 GMT+0600 (Bangladesh Standard Time)
2 User Login: Logged in as 'testuser1' at: 22:56:17 GMT+0600 (Bangladesh Standard Time)
3
```

Figure 5.15: Login Logs.

```
audit.log M X
backend > audit.log
1 'getModifyQueue' initiated by user 'testuser1' at: 23:05:47 GMT+0600 (Bangladesh Standard Time)
2 'modifyNID' initiated by user 'testuser1' at: 23:07:44 GMT+0600 (Bangladesh Standard Time)
3 'getModifyQueue' initiated by user 'testuser1' at: 23:07:47 GMT+0600 (Bangladesh Standard Time)
4 'getModifyQueue' initiated by user 'testuser1' at: 23:08:23 GMT+0600 (Bangladesh Standard Time)
5
```

Figure 5.16: Action Logs.

## Access Review:

This module will gather all the critical users in the system and remove them accordingly. Critical users are flagged by their expired access to resources and unauthorized access too. With a simple click of button, the backend will gather all the criticals, remove them and notify the admin.

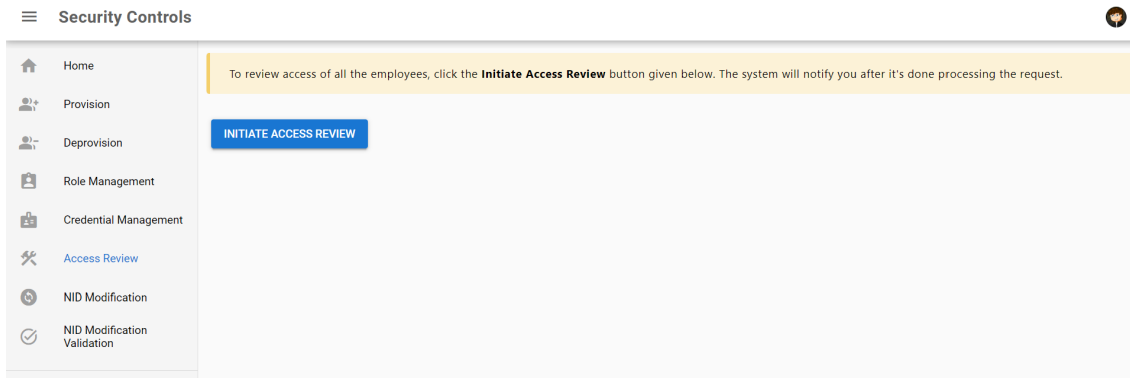


Figure 5.17: Frontend view of Access review.

## Segregation of Duties (SoD):

This is not actually a module, but rather it is a security concept. We used this concept to divide the task of NID modification into two parts and assigned the task to two different officials. This is merely a suggestive structure to implement inside the organization to prevent NID forgery. The task depends on two officials and for that reason, it will be harder to forge NIDs just by a corrupted official. One modification official will simply input the NID information in the system, but it will be directly added to a queue. Another validation official will further verify the data and validate with other sources and accept the modification request or reject it. The following pictures show a demo of the structure which can be implemented with further modifications.

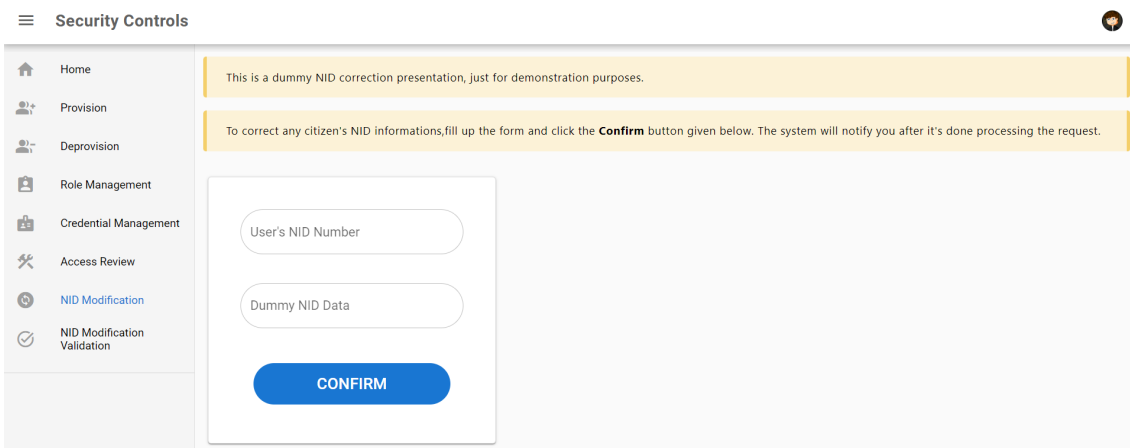


Figure 5.18: Figure: Frontend view of NID Modification (Demo).

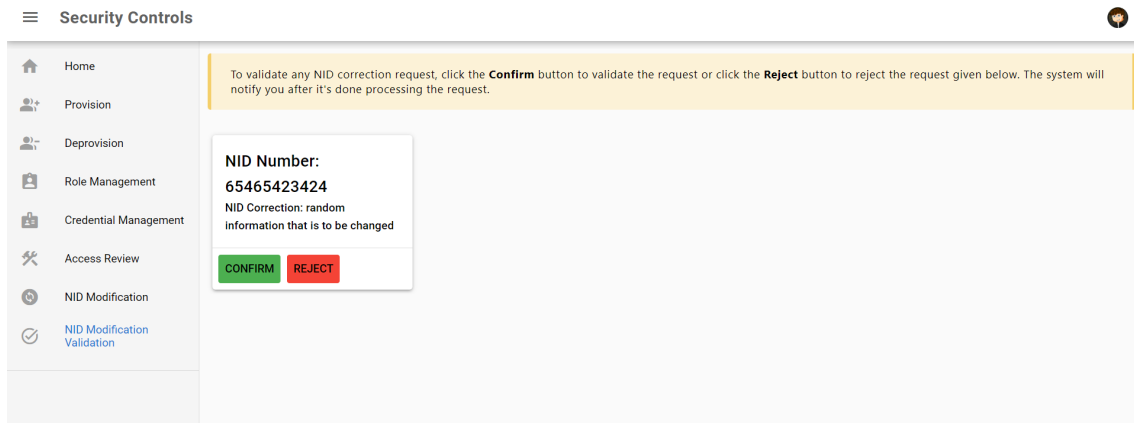


Figure 5.19: Frontend view of NID Modification Validation (Demo).

### Reporting and Analytics:

This module will handle different data in the system while analyzing and creating meaningful reports about the state of the system. It can be used in many ways and the reports will have great decision making factors to help decide different things in the organization. For the lack of information, time and resources available to us about how the organization works, we couldn't implement this module for now.

# Chapter 6

## Result and Analysis

Since each security control in our model is created as a separate unit, we determined it would be preferable to utilize the unit testing approach to thoroughly test the modules, obtain thorough findings, and evaluate the entire model. We tested to see if each module operated as a separate entity and recorded all of the findings. The 'jest' library was used to test all the modules and we created separate test suites for each of the modules.

```
> security-controls@1.0.0 test
> jest --runInBand --forceExit

PASS   TestCode/rbac.test.js (6.238 s)
PASS   TestCode/mfa.test.js (5.605 s)
PASS   TestCode/cm.test.js (5.684 s)
PASS   TestCode/em.test.js (7.83 s)
PASS   TestCode/el.test.js
PASS   TestCode/ar.test.js

Test Suites: 6 passed, 6 total
Tests:      23 passed, 23 total
Snapshots:  0 total
Time:       25.756 s, estimated 30 s
Ran all test suites.
```

Figure 6.1: Testing Result of the modules.

### Multi-Factor Authentication :

As seen in the module’s test-cases, we have tested the module’s ability to detect valid and invalid login attempts and also the ability to efficiently sending the OTP on valid user credentials input and the module passed all those tests perfectly.

Test Case ID	Test Scenario	Test Case	Test Data	Expected Result	Actual Result	Status
MFA-001	Checking Multi-Factor Authentication Functionalities	Logging in with valid login credentials	Valid Email: "testuser1@gmail.com" Valid Password: "testuser1"	A message should be returned saying "OTP has been sent to user's email"	Returned a message saying "OTP has been sent to user's email"	Passed
MFA-002		Logging in with incorrect password	Valid Email: "testuser1@gmail.com" Incorrect Password: "incorrect"	An error should be returned with the message "Incorrect Password"	Returned an error with the message "Incorrect Password"	Passed
MFA-003		Logging in with invalid login credentials	Invalid Email: "nonexisting@gmail.com" Invalid Password: "nonexisting"	An error should be returned with the message "Invalid User"	Returned an error with the message "Invalid User"	Passed
MFA-004		Sending OTP on valid login	Valid Email: "testuser1@gmail.com"	The email and the generated OTP should be returned	Returned the email and the generated OTP	Passed

Table 6.1: Multi Factor Authentication

### Credential Management:

As seen in the module's test-cases, we have tested the module's ability to correctly change a user's email and password credentials. We have also tested the ability to detect invalid inputs given to the module and the module passed all those tests perfectly.

Test Case ID	Test Scenario	Test Case	Test Data	Expected Result	Actual Result	Status
CM-001	Checking Credential Management Functionalities	Changing a valid user's email address	Current email: "testuser1@gmail.com" Email to be set: "testuser2@gmail.com"	Both emails get returned	Returned both emails	Passed
CM-002		Changing an invalid user's email address	Current email: "nonexisting1@gmail.com" Email to be set: "nonexisting2@gmail.com"	An error should be returned with the message "User not found"	Returned an error with the message "User not found"	Passed
CM-003		Changing a valid user's password	Valid email: "testuser1@gmail.com"	The email and a new password should be returned	Returned the email and a new password	Passed
CM-004		Changing an invalid user's password	Invalid email: "nonexisting1@gmail.com"	An error should be returned with the message "User not found"	Returned an error with the message "User not found"	Passed

Table 6.2: Credential Management

### Role-Based Access Control:

As seen in the module's test-cases, we have tested the module's ability to correctly create a permission or a role or delete a role and also tested the ability to assign those roles and even remove them. We have also tested the ability to detect invalid inputs given to the module and the module passed all those tests perfectly.

Test Case ID	Test Scenario	Test Case	Test Data	Expected Result	Actual Result	Status
RBAC-001	Checking Role-Based Access Control Functionalities	Creating a assignable role permission	Name: "random name" Ability: "can do this"	The created permission with the name and ability should be returned	Returned the created permission with the name and ability	Passed
RBAC-002		Creating a assignable role	Name: "random name" Permissions: An array of permissions	The created permission with the name and permissions should be returned	Returned the created permission with the name and permissions	Passed
RBAC-003		Deleting a role	Name: "random name"	Should return 'True'	Returned 'True'	Passed
RBAC-004		Assigning a role to a valid user	Valid user email: "testuser1@gmail.com" Role: 'admin'	The user with the assigned role should be returned	Returned the user with the assigned role	Passed
RBAC-005		Assigning a role to an invalid user	Invalid user email: "nonexisting@gmail.com" Role: 'admin'	Returned an error with the message "Could not assign the role"	Returned the user with the assigned role	Passed
RBAC-006		Removing a role from a valid user	Valid user email: "testuser1@gmail.com" Role: 'admin'	The user with the removed role should be returned	Returned the user with the removed role	Passed
RBAC-007		Removing a role from an invalid user	Invalid user email: "nonexisting@gmail.com" Role: 'admin'	An error should be returned with the message "Could not remove the role"	Returned an error with the message "Could not remove the role"	Passed

Table 6.3: Role-Based Access Control



### Entitlement Management:

As seen in the module's test-cases, we have tested the module's ability to correctly assign and remove an entitlement from a user. We have also tested the ability to detect invalid user data given to the module and the module passed all those tests perfectly.

Test Case ID	Test Scenario	Test Case	Test Data	Expected Result	Actual Result	Status
EM-001	Checking Entitlement Management Functionalities	Assigning an entitlement to a valid user	Valid user email: "testuser1@gmail.com" Role: 'admin' Period: 24 hours	The user with the assigned role for a period of 24 hrs should be returned	Returned the user with the assigned role for a period of 24 hrs	Passed
EM-002		Assigning an entitlement to an invalid user	Invalid user email: "nonexisting@gmail.com" Role: 'admin' Period: 24 hours	An error should be returned with the message "Could not assign the entitlement"	Returned an error with the message "Could not assign the entitlement"	Passed
EM-003		Removing an entitlement from a valid user	Valid user email: "testuser1@gmail.com" Role: 'admin'	The user with the removed role should be returned	Returned the user with the removed role	Passed
EM-004		Removing an entitlement from an invalid user	Invalid user email: "nonexisting@gmail.com" Role: 'admin'	An error should be returned with the message "Could not remove the entitlement"	Returned an error with the message "Could not remove the entitlement"	Passed

Table 6.4: Entitlement Management

### Access Review:

As seen in the module's test-cases, we have tested the module's ability to correctly all the critical users from the system and the module passed the test perfectly.

Test Case ID	Test Scenario	Test Case	Test Data	Expected Result	Actual Result	Status
AR-001	Checking Access Review Functionalities	Removing Critical users	Critical Users: An array of users	The critical users should be returned after removal	Returned the critical users	Passed

Table 6.5: Access Review

### Event Logging:

As seen in the module's test-cases, we have tested the module's ability to correctly log all the login, logout and initiated actions by any user in the system and the module passed all those tests perfectly.

Test Case ID	Test Scenario	Test Case	Test Data	Expected Result	Actual Result	Status
EL-001	Checking Event Logging Functionalities	Logging an action	Action: "Access review" Initiator: 'testuser1' Time: Initiation time	The action's logged text should be returned	Returned the user with the action's logged text	Passed
EL-002		Logging a successful login	User: 'testuser1' Time: Initiation time	The login's logged text should be returned	Returned the user with the login's logged text	Passed
EL-003		Logging a successful logout	User: 'testuser1' Time: Initiation time	The logout's logged text should be returned	Returned the user with the logout's logged text	Passed

Table 6.6: Event Logging

# Chapter 7

## Conclusion

Security models like ours are used to limit the risk to the public's data in an information system by eliminating any compromising situation. That means, despite all the research and security solution models used to defend e-government systems on a daily basis, the risk of data compromise still exists, it might only be partially tackled. No matter how much we try to come up with a better solution, There will always be a human factor. Human behavior or emotions are not easily controllable and we have very little control over these. This factor has been a huge limitation to almost all technologies and our proposed work is no exception. Our work was focused on segregation of duties, so that no one person or rather a human has complete control over any important and sensitive task. We tried to think of as many unique approaches to fully eradicate this issue as possible, but we got the idea that the issue will always remain. From the start of our research, we have referred to recent examples of such incidents, where employees from the organization themselves were behind all the illegal activities. This proves that even strict security protocols can be ignored by the insiders and this poses the greatest threat according to most security personnels. But yes, it is surely possible to narrow down the occurrences by tightening loose ends. As we can not control human behavior, we come up with new and more advanced ways to enforce these security policies, therefore, there are endless opportunities for future research in this path. Although, there has been a shortage of research that attempts to get into the nitty-gritty of identity governance and administration. With our outstanding insights and the creation of a security model based on IGA, this research aims to address this gap and plans to further extend the model with more advanced techniques/controls in the coming future.

# Bibliography

- [1] Ministry of science and information & communication technology and government of the people's republic of bangladesh, "bangladesh ict policy 2002," en, sdnbd.org, Oct. 2002. [Online]. Available: <http://sdnbd.org/sdi/issues/IT-computer/itpolicy-bd-2002.htm>.
- [2] W. Shi, "Download limit exceeded," en, *citeseerx.ist.psu.edu*, Feb, vol. 10, 2006, accessed May 19, 2022). [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.934.1740&rep=rep1&type=pdf>.
- [3] B.I.P.S.S., *Cyber security — the emerging threat landscape*, en, Jan. 2012.
- [4] L. Sun., H. Wang, J. Soar, and C. Rong, "Purpose based access control for privacy protection in e-healthcare services," en, *core.ac.uk*, vol. 7, Nov. 2012, [Online]. Available: [Online]. Available: <https://core.ac.uk/reader/11050121>.
- [5] C. K. Wangwe, M. M. Eloff, and L. Venter, "A sustainable information security framework for e-government – case of tanzania," cs, *Technological and Economic Development of Economy*, vol. 18, no. 1, pp. 117–131, Apr. 2012. DOI: 10.3846/20294913.2012.661196..
- [6] Y. Alkhorayef, "National id cards," en, *International Journal of Computing Science and Information www.ijcsit.org*, vol. 1, no. 02, p. 2, 2013, [Online]. Available: [Online]. Available: <http://ijcsit.org/IJCSIT-iss2-p7.pdf>.
- [7] M. Gustafsson and W. Elin, "Safe online e-services building legitimacy for e-government. a case study of public e-services in education in sweden," en, *JedDEM - eJournal of eDemocracy and Open Government*, vol. 5, no. 2, pp. 155–173, Mar. 2014. DOI: 10.29379/jedem.v5i2.223..
- [8] A. M. Maruf, M. R. Islam, and B. Ahamed, "Emerging cyber threats in bangladesh: In quest of effective legal remedies," en, *Northern University Journal of Law*, vol. 1, pp. 112–124, Apr. 2014. DOI: 10.3329/nujl.v1i0.18529..
- [9] O. A. Ali, T. M. Wahbi, and I. ' . M. Osman, "E-government security models," en, *International Journal of Computer Applications Technology and Research*, vol. 5, no. 7, pp. 439–442, Jul. 2016. DOI: 10.7753/ijcatr0507.1004..
- [10] M. Alamgir and M. J. Khan, "Nid forgery: Ec officials compromising server security," en, *The Daily Star*, Sep. 15, 2020, accessed May 19, 2022). [Online]. Available: <https://www.thedailystar.net/country/news/nid-forgery-ec-officials-compromising-server-security-1961893>.

- [11] A. Foyez, “Ec struggling to check nid forgery,” en, in *New Age — The Most Popular Outspoken English Daily in Bangladesh*, Sep. 25, 2020. [Online]. Available: <https://www.newagebd.net/article/117208/ec-struggling-to-check-nid-forgery>.
- [12] U.N.B., “Nid forgery: 5 gang members held in city,” no, *Dhaka Tribune*, Sep. 13, 2020. [Online]. Available: <https://www.dhakatribune.com/bangladesh/crime/2020/09/13/nid-forgery-5-gang-members-held-in-city>.
- [13] M. H. Alruwies, S. Mishra, M. Abdul, and R. Alshehri, *Identity governance framework for privileged users*, en, researchgate.net, Sep. 2021. [Online]. Available: [https://www.researchgate.net/publication/354879350\\_Identity\\_Governance\\_Framework\\_for\\_Privileged\\_Users](https://www.researchgate.net/publication/354879350_Identity_Governance_Framework_for_Privileged_Users).
- [14] R. Hill, “Identity governance & administration 2021,” en, *KuppingerCole, Jun*, vol. 29, 2021, accessed May 19, 2022). [Online]. Available: <https://www.kuppingercole.com/research/lc80516/identity-governance-administration-2021>.
- [15] B. Lee, *What is identity governance and administration (iga)?* en, Aug. 5, 2021.
- [16] S. N. Deekue, “A strategic framework for e-government security: The case in nigeria,” en, in *uobrep.openrepository.com, Apr. 2016*, [Online]. Available: Accessed, May 19, 2022. [Online]. Available: <https://uobrep.openrepository.com/handle/10547/622496>.
- [17] R. Albrahim, H. Alsalamah, S. Alsalamah, and M. Aksoy, *Access control model for modern virtual e-government services: Saudi arabian case study*, en, semantic scholar.org, 2018. [Online]. Available: <https://www.semanticscholar.org/paper/Access-Control-Model-for-Modern-Virtual-Services%3A-Albrahim-Alsalamah/ebb010ac868b6bb721a9db5d2bc33e24cf48895b>.
- [18] Bangladesh ICT Division, *E-government master plan for digital bangladesh*, en, bcc.portal.gov.bd. [Online]. Available: [https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/publications/3f9cd471\\_9905\\_4122\\_96ee\\_ced02b7598a9/2020-05-24-15-54-43f3d2b8b4523b5b62157b069302c4db.pdf](https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/publications/3f9cd471_9905_4122_96ee_ced02b7598a9/2020-05-24-15-54-43f3d2b8b4523b5b62157b069302c4db.pdf).
- [19] G. Botchwey, *E-governance and cybersecurity: User perceptions of data integrity and protection in ghana*, en, researchgate.net, Mar. 2018. [Online]. Available: [https://www.researchgate.net/publication/323848012\\_E-Governance\\_and\\_Cybersecurity\\_User\\_Perceptions\\_of\\_Data\\_Integrity\\_and\\_Protection\\_in\\_Ghana](https://www.researchgate.net/publication/323848012_E-Governance_and_Cybersecurity_User_Perceptions_of_Data_Integrity_and_Protection_in_Ghana).
- [20] “Iam vs iag: What’s the difference,” en, *Tools4ever*, accessed May 19, 2022). [Online]. Available: <https://www.tools4ever.com/blog/iam-iga-difference>.
- [21] Z. Liaquat and M. Mavis, “How strong is financial cybersecurity in bangladesh?” es, *Dhaka Tribune*, vol. 10,
- [22] R. M. Reffat, *Developing a successful e-government*, en, citeseerx.ist.psu.edu. [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.505.4177&rep=rep1&type=pdf>.
- [23] G. White and W. A. Conklin, *E-government and cyber security: The role of cyber security exercises*, en, researchgate.net, Feb. 2006. [Online]. Available: [https://www.researchgate.net/publication/4216146\\_e-Government\\_and\\_Cyber\\_Security\\_The\\_Role\\_of\\_Cyber\\_Security\\_Exercises](https://www.researchgate.net/publication/4216146_e-Government_and_Cyber_Security_The_Role_of_Cyber_Security_Exercises).

- [24] Z. Zhou and C. Hu, *Study on the e-government security risk management*, en, citeseerx.ist.psu.edu, 2008. [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.385.6270&rep=rep1&type=pdf>.