**UNIVERSITY OF ZIMBABWE** 

FACULTY OF COMPUTER ENGINEERING, INFORMATICS AND

COMMUNICATION

DEPARTMENT OF COMPUTER SCIENCE

**Project Proposal: Secure online National ID booking and retrieval system**

PARTIAL FULFILLMENT OF THE DEGREE OF BACHELOR OF SCIENCE CLOUD COMPUTING AND IOT

**STUDENT NAME: KANDEYA GODFREY T**

**PROGRAM: HCC**

**REG NUMBER: R219420M**

**SUPERVISOR: MR. DEVE**

Table of Contents

[**2.1 Literature Review 2**](#_c90q0o779xn9)

[2.1.0 Introduction 2](#_pbnmq4o4zkja)

[2.2 Theoretical Framework 3](#_feizxhx2cgql)

[2.3 Research Methodology 3](#_7tb5b2c73ha)

[2.4 Methodological Approach 3](#_p7ma32se7wxj)

[2.5 Data Structure 4](#_p0zybx9tqcm7)

[2.6 Description of Methods of Data Collection 4](#_j27g4z406ftb)

[2.7 Description of Methods of Analysis of Data 5](#_qtdwjr4zyor9)

[2.8 Evaluation & Justification of Methodological Choices 5](#_zdzc02rm1da8)

[2.9 Resource Requirements 6](#_t26ezjjarqtr)

[3.0 Software Requirements 6](#_mg82nut135uu)

[3.1 Hardware Requirements 7](#_vro6cjmx6yhs)

[3.2 Functional and Network Requirements 7](#_n1re8kuznz7c)

[3.3 Functional Requirements 7](#_5h0l195bvj46)

[3.4 Network Requirements 8](#_gtaxzfqe8sux)

[3.5 Non-Functional Requirements 8](#_tga3g4vaa14l)

[3.6 Modelling Diagrams 9](#_glww5pm285bz)

[3.7 Software Projects 10](#_a325o0lq7z67)

[3.8 Historical Context 10](#_4cie9en246ug)

[3.9 Key Studies and Their Findings 10](#_df2f30s68shs)

[4.0 Methodological Approaches 11](#_p956kc4ceggg)

[4.1 Controversies and Debates 12](#_eox226y806en)

[4.2 Synthesis and Evaluation 12](#_yjmshsv5iyw1)

[4.3 Project Plan 13](#_b7otfse0byds)

[4.4 Conclusion 14](#_3evqrekcqax6)

[References 15](#_dlz13vx511rm)

### 

### 

### 2.1 Literature Review

#### 2.1.0 Introduction

National identity systems can either be the lynchpin of every citizen's access to all basic services and full participation in economic life or they can paralyze it. In Zimbabwe, to get a national ID entails laborious and time-consuming in-person visits that stand in the way of receiving much-needed services like healthcare, education, and even financial support, especially in areas that are rural or otherwise underserved. Apart from being inefficient, the traditional ID process in Zimbabwe lacks adequate security to protect against fraud and identity theft (Deloitte, 2017; World Bank, 2018), furthering the risks to citizens' personal information. This digital ID project is one such transformative solution in the form of an online ID booking and retrieval system that seeks to bridge these gaps in access. The ambition is to incorporate an easy-to-use, user-friendly interface that will digitally engage all Zimbabweans with government services, thus supporting modernization of the economy and improvement in government transparency.

#### 2.2 Theoretical Framework

This project is based on three critical theoretical frameworks that provide its foundation: Information Security Theory, Zero Trust Architecture, and E-Government Theory(Whitman & Mattord, 2018). These will be the basis for a detailed, secure digital ID system to meet the needs of Zimbabwe.

The theory of Information Security has something to do with securing confidentiality, integrity, and availability of data-all important aspects in the Zimbabwean digital sphere. Strong encryption and access control, coupled with proper management of data, all form part of how confidential data such as biometric information are kept and transmitted; data protection regulations fall under this theory.

Furthermore, Zero Trust Architecture incorporates the philosophy of "never trust, always verify." This philosophy certainly comes in handy and always applies to the cybersecurity challenges facing Zimbabwe today. The basic components, as extracted from the ZTA framework, are that every access request in the systems goes through multi-factor authentication with dynamic access control; thus, only the intended users can access the data. Micro-segmentation and Single Packet Authorization reduce data exposure risks and unauthorized access in this architecture.

E-Government Theory underlines the role of digital platforms in improving the delivery, transparency, and access of government services. This theory considers the system design to be inclusive, so the full range of end-users, independent of their level of digital skill, are able to use the platform. This is in accordance with global best practices in e-government and considers ways to maximize user experience and outreach to underserved populations, hence making the digital transformation inclusive for Zimbabwe. (Heeks 2006).

#### 2.3 Research Methodology

#### 

This section highlights the research methodology chosen for the purpose of creating a secure and user-friendly digital ID booking and retrieval system. The method employs surveys and systems logs to assess user satisfaction and system performance. The integration of these data sources makes it possible to carry out an in-depth examination of the system usability, security, and functionality.

#### 2.4 Methodological Approach

For the purposes of this project, the methodological approach is based on the agile development framework. Agile’s iterations are vital through feedback and improvement which is very important when creating a safe and user-friendly digital identity management system. This allows for incorporating regular enhancements and dealing with functionality and security issues that may arise during the development process.

The agile method encourages the use of design principles adapted to user needs, making surveys and user logs a priority for audience feedback. This facilitates the incorporation of real-time user input and system performance data for the purposes of ensuring both user satisfaction and operational effectiveness of the system in practical usage.

#### 2.5 Data Structure

The particular project needs many data types to make certain that the developing, testing, and polishing of the ID system is done comfortably and effectively:

1. User Data

It can be presented as questionnaires filled by the users who give an opinion about the ease of use, accessibility, and general feeling about the reviewed system. This comes in handy when analyzing users from different profiles how they utilize the system and assessing the problematic aspects.

1. Performance Data

It includes system generated information that is used to monitor how the system performs in terms of back end performance metrics, error rates, response times and server usage levels. This type of data is important to diagnose and resolve performance issues and security threats as well as other overhauls that are needed.

1. Biometrics

This comprises sensitive details like fingerprints or e-signatures (as obtained through 3 rd party API integrated methods for safe collection of biometric samples) managed by the system. This type of information is extremely important for user verification, thus is secured and encrypted prior to storage in compliance with regulatory requirements.

#### 2.6 Description of Methods of Data Collection

Data collection methods are designed to capture insights from users and measure the performance of the system:

1. Surveys

Objective Surveys are carried out on a range of users in order to obtain both qualitative and quantitative information pertaining to the usability, accessibility, and features of the system.

Coverage/Contents Surveys cover ease of use, effectiveness of the system’s mobile version, average response time, and perceived data’s safety.

Administration The surveys are carried out via the internet to access both urban and rural users, hence the need for all the respondents. The responses help to shape the changes that will be made on the user interface and the experience.

1. System Logs:

Objective System logs are utilized to gather performance metrics on the back end by looking at response time, server load, errors, etc.

Coverage/Contents Logs give updated information on real-time challenges such as attacks, performance and data-related issues.

Administration Logs are generated by back-end surveillance systems on a continuous basis and reviewed annually to avert unplanned downtimes and breaches of the system.

#### 2.7 Description of Methods of Analysis of Data

The focus of choosing data analysis methods available is to derive positive changes or conclusions from the collected raw data.

1. Statistical Analysis

Objective technique is used on the retrieved questionnaire data in which respondent’s comments on the tools usability, accessibility and satisfaction are collated.

Quantitative analysis (derived from rating scale responses) utilizes descriptive statistics for trend analysis while qualitative responses are processed through coding them and sorting into groups to find their themes.

1. Performance Analysis

Performance analysis involves examining the system’s logs in order to obtain such metrics as response time, error rate and load balancing.

Logs are assessed through application associated monitoring services (for instance, AWS Cloud Watch) in order to enhance performance. This assessment will also outline the performance statuses of individual backend elements that may need enhancements.

1. Vulnerability Assessment

Analysis of biometric information focuses on both the potential security risks and the legislation.

Biometric information in hashed files is periodically accessible and controls implemented to prevent prohibited access to them enforced with systems such as KMS.

#### 2.8 Evaluation & Justification of Methodological Choices

The evaluation of the selected methodologies is carried out as follows.

1. Agile Development

The essence of Agile is based on continuous iteration and hence system can be improved in terms of user feedback and system performance over short periods of time. This approach is particularly useful for the developing project with regards to large amount of sensitive data and varied group of users as it allows for changes to user needs or security risks to be incorporated brief.

1. Survey-Based Data Collection

Surveys draws an important user view with respect to the usability and access of the system in question, particularly for a project that has a varied target group. In this case, surveys facilitate the targeting of users with respect to varying levels of digital literacy.

1. Log-Based System Performance Evaluation

System logs ensure the provision of data on the relative performance of the system and also on any security breaches log therefore enabling the optimization of the system in real time. This method is pertinent in the control of system management processes that deal with the backend and the provision of security and dependability of the system.

#### 2.9 Resource Requirements

In this section, the software and hardware resources necessary for the implementation of the digital ID system are detailed. Each requirement aids different stages of the project from development to system deployment and subsequent performance.

#### 3.0 Software Requirements

1. Frontend Development

React.js - A framework written in JavaScript and used to build fast, interactive user interfaces for different devices that allows users to interact with the interface.

HTML/CSS/JavaScript - the fundamental technologies of the web which aim to build and layer a beautified interactive user interface. They ensure accessibility as well as reactivity especially in the case of mobile applications alongside desktop applications.

1. Backend Development

Python/Django -The primary backend framework for managing application core logic, user accounts, and data repositories. Given its support for applications that are highly available, secure and scalable, Django encourages complex applications development.

1. Database

MySQL - A free, open-source, relational database management system designed for saving personal profiles and biometrics. Sensitive information will be encrypted in accordance with security and privacy standards.

1. Cloud Services

AWS CodePipeline An automation service for expanding, testing, and deploying the platform. It shall be used together with Docker to ensure that the development, testing and production environments do not differ in their configurations.

AWS Elastic Beanstalk (or EC2) - The use of the clouds for facilitation of enhanced scalability and availability. Deployment is made easy with Elastic Beanstalk, while one has EC2 for server control and management an advanced option.

Aws S3 - A secure and scalable filing system for user-uploaded documents such as id photos with in built encryption and access control features.

Business Logic Management and Virtual Task Executor:

Redis Cache -To cache warm data and reduce load on the database.

Task Queue Management - For background tasks such as biometric data collection and status notifications to the users.

Infrastructure, CI/CD Pipeline and Application Deployment:

GitHub Actions - Automated testing, linting and security checks on code push.

In AWS CodePipeline: N deploys pipeline for…

#### 3.1 Hardware Requirements

1. Servers

Cloud Servers (AWS EC2/Elastic Beanstalk) - Deployed for the backend application and its associated services to provide adequate scaling and high service availability.

Database Server -An exclusive instance, which is a MySQL database file, will be used to keep the personal and biometric data securely in an encrypted form.

1. Biometric Scanners:

Fingerprint Scanners - these are technical devices that are used to collect biometric information and to authenticate that information. These scanners are indispensable for secure identity management.

1. User Devices

Mobile phones Table computers and laptops This hardware is used to assess the system’s accessibility on varied devices and its compatibility and user-friendliness.

#### 3.2 Functional and Network Requirements

#### 3.3 Functional Requirements

These are the functional requirements, which this system is required to comply with.

1. User Registration and Login

Allows users to register and log in to their identification profiles with an advanced level of security by way of multi-factor authentication.

1. Biometric Recording

Utilizes a fingerprint or facial scan of the users with the help of 3rd party services for securing the capture of sensitive information of the users.

1. Admin Control Panel

Empowers government officials with the capability to oversee the operations of ID request processing, system operations, performance metrics, and other relevant information.

1. Notifications

Provide a secure means of communicating with clients wishes informing them on the progress of application and especially gender based id request’s status.

#### 3.4 Network Requirements

1. Ensured Internet Access

Provides a secure way of transmitting information by encrypting the users, the application, and the aws infrastructure using ssl or ts, layered security.

1. Firewall Protection

There is a layer of security that acts as a barrier the user and the databases in the system to restrict unwanted access and thus protect the system

1. Encryption Protocols

There are two main encryption standards applied in the network, ssl/tls for transmission of data information and aes for storage encryption of data.

#### 3.5 Non-Functional Requirements

1. Performance

It is expected of the system that it can accommodate many users at the same time without unreasonable delay.

1. Reliability

System availability shall be at least 99% and regular backups will be taken so that data loss will not occur.

1. Scalability

There has to be the provision for extending the system i.e. adding new ID types or increasing the number of users when necessary.

1. Usability

Access to and interaction with interfaces must be available, quick and facile to use for persons of different technological literacy.

#### 3.6 Modelling Diagrams

1. Use Case Diagram

It displays major activities such as ID application, capturing biometric data, processing of application by administrators, and notifying updates.

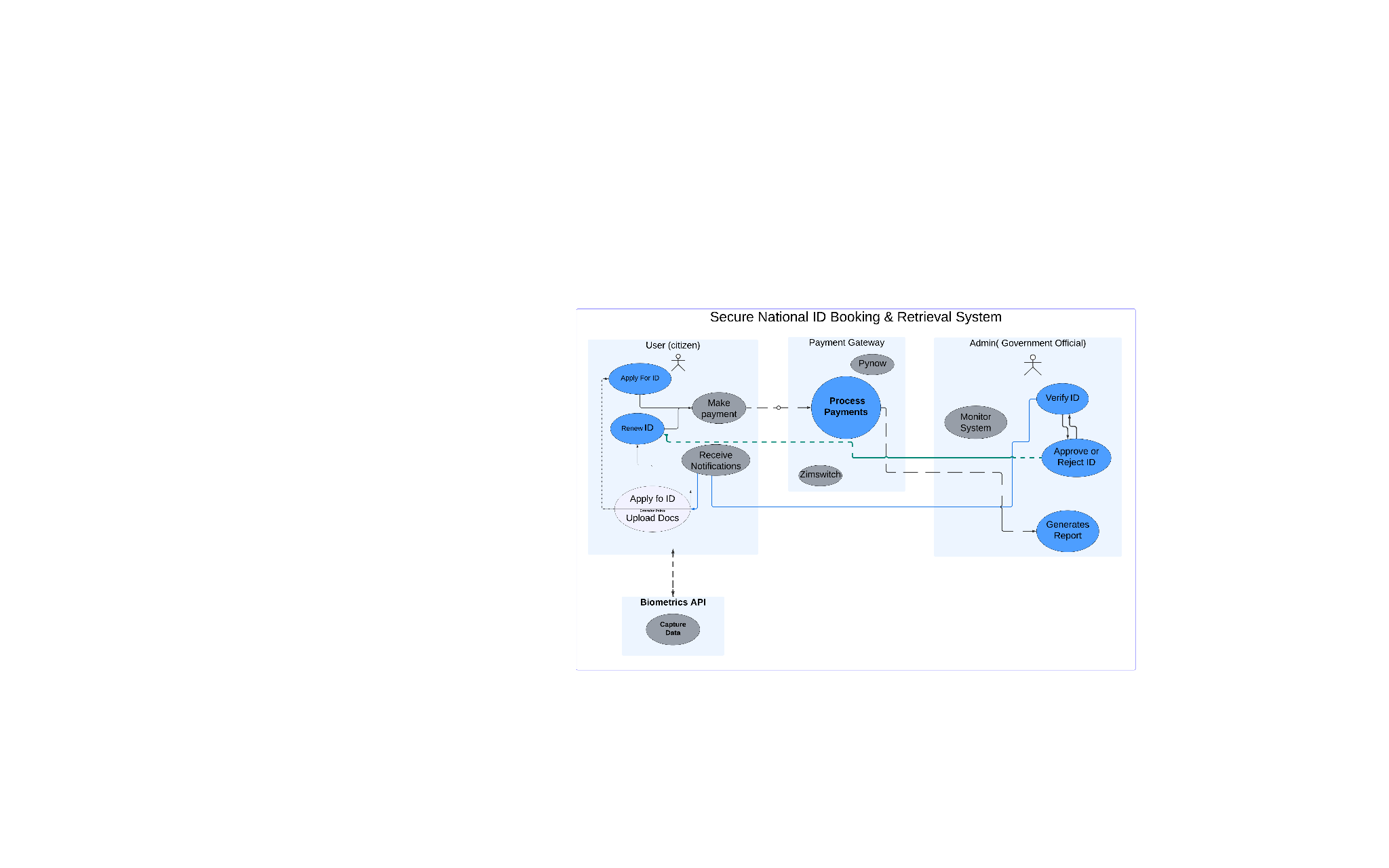
****

Fig 2.6

#### 3.7 Software Projects

1. Frontend-Backend Communication

React and Django are connected using GraphQL for optimal data transfer and faster interface response.

1. Biometric Data Handling

APIs for biometric capture are integrated and secured considering confidentiality and privacy issues associated with the data.

1. AWS Integration

The AWS services enable scalability, security, and optimal resource management in the course of the development and deployment processes.

#### 

#### 3.8 Historical Context

Traditionally, Zimbabwe's ID system has been paper-based, where one has to physically appear to be registered or renew their documentation, hence creating barriers in rural setups. Global experiences drawn from countries such as Estonia and India indicate that digital ID systems address some of these barriers(Gelb & Clark, 2013); thus, there are lessons that need to be drawn for Zimbabwe. Examples include Estonia's e-ID system, deploying heavy encryption and multi-factor authentication. The result has been a drastic reduction in identity fraud and a citizenry enabled to access healthcare, banking, and voting services online(Deloitte, 2017). Similarly, India's Aadhaar system has greatly helped increase the rate of access to services among its over-one-billion citizens. This is despite the criticism of data privacy that the system has come under. This dual perspective allows Zimbabwe to be better placed to understand both the benefits of digital ID and its various challenges, underlining how necessary it is to balance accessibility against data protection.

#### 3.9 Key Studies and Their Findings

Studies of digital identification systems show high efficiency and greater accessibility; at the same time, research points to several challenges in the contexts of cybersecurity and privacy.

Accompanying benefits from this are: India's Aadhaar decreased service queue waits by 25% and increased the verification speed of documents, showing the efficiency that digital IDs can bring to large-scale systems(Banerjee & Duflo, 2019). Indeed, cost-effectiveness is among the benefits achieved by the Estonian e-ID system, saving the government millions of euros annually due to reduced times of processing(Madise & Martens, 2006). From this, the indication would be for Zimbabwe that digital ID makes government service delivery faster and more efficient to citizens and administrative staff alike.

Challenges - cybersecurity still appears to be a concern. It is reported that the Aadhaar system suffered several breaches due to which there was a risk of misusing sensitive data on citizens(World Bank, 2018; Gelb & Metz, 2018). Thus, to handle such risks in Zimbabwe, the proposed project shall apply a very robust framework- Zero Trust by Design [ZTBD], based on the principles of stringent access control, regular authentication, and encryption of biometrics. This, in addition, underlines the need for security at multiple levels, verification through biometrics, data encryption, among others to avoid data misuse and unauthorized access, which is critical in the system design in Zimbabwe.

#### 4.0 Methodological Approaches

Various research strategies were employed in the wrote up of the literature on secure digital identification systems. Typical methods consist of the use of case study, comparative study and technical study.

Case Studies: Two of the most important digital identity-related projects, those of Estonia and India, have crucial lessons to teach(Gelb & Clark, 2013). While in Estonia, end-to-end encryption has been put in place, thus necessitating the existence of a robust security mechanism and centralization of management of data, India's Aadhaar system on the other hand, puts emphasis on the need for biometrics. It is these examples that have so far guided the strategy Zimbabwe adopted, which is clear from the sound examples of appropriate data shielding and the principle of sectional expansion.

The Cross–Country Comparative deals with the common data privacy problem faced by all researchers and encourages the modification of some (widely researched) methods, such as micro-segmentation and encryption protocols, to the Zimbabwe infrastructure. In this context, the comparison analysis emphasizes the notion of security systems development that is not only effective but also elastic, balancing the elasticity with the offered protection of the information.

Security Technical Analysis: A difference of perspective is in the application of Zero Trust as the strategy incorporates controlling access to the different layers of Zimbabwe ID system and change of authentication at all levels. Other security aspects such as Single Packet Authorization and 24 hour supervision play a crucial role in preventing security breaches and content theft while ensuring that the law is upheld (Whitman & Mattord, 2018).

#### 4.1 Controversies and Debates

The application of information technology in identity management raises ethical issues – particularly regarding privacy, surveillance, and access, which are of concern to Zimbabwe as well(Zwitter, 2014).

Privacy and Surveillance: With the implementation of such systems, the authorities are provided with the ability to surveil the population due to the centralisation of data systems. The privacy infringement tendencies associated with the utilisation of the Aadhaar system in India are proof of the dangers of data collection at a national level. In Zimbabwe, it will be important for the implementation of Privacy by Design where data minimization and consent are key due to social challenges and the need for trust.

Digital Inequalities: Challenges arise in relations to system accessibility due to the disparity in levels of Internet usage and digital literacy between town and countryside. Given this, Zimbabwe’s ID system will have to provide for offline data submission and mobile verification for those without internet connection, if inclusivity is to be promoted. With this strategy, citizens will be able to access digital ID services irrespective of their region, even if they have no connectivity.

Ethical Safeguards: As a way to counter ethical challenges, an appropriate user-friendly Data Protection Act could be put in place in Zimbabwe’s digital ID system(World Bank, 2018). This helps in alleviating public apprehension regarding data abuse and is consistent with the ethical standards of digital ID systems.

#### 4.2 Synthesis and Evaluation

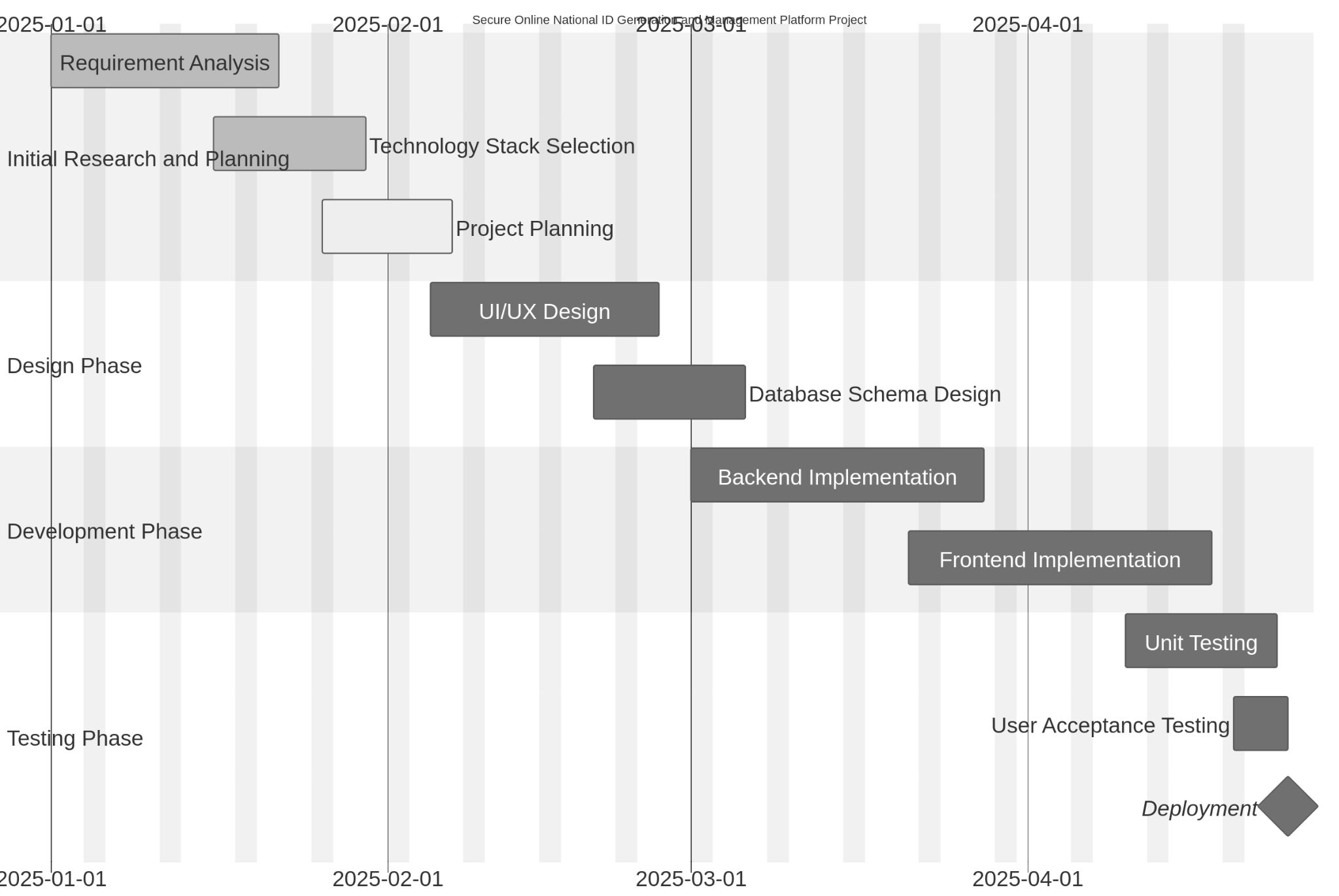
Based on the research papers we examined, all point the way for the possibility of establishing a safe and comprehensive digital ID system in Zimbabwe, outlining a number of helpful uses.

Defense in Depth: Incorporating various elements such as encryption, micro-segmentation and strong authentication creates a robust ID system that protects sensitive content/ information. This encourages some additional threats protection and compliance with the data protection policies of Zimbabwe.

Continuous Monitoring and Adaptive Security: With this, current threats can be obliterated by supervision and availability of security policies that employ flexible resources. For instance, in case of suspect login activity, the system may prompt for additional authentication thus preventing unauthorized access and fraud.

Inclusive Design for Accessibility: It is paramount that the system does not just “work” but is also designed for, and used by, people with different levels of digital literacy. Another example would be for users from the rural areas who are surge to mobile based designs or safe community wide enrollment facilities that would enhance access to the largely rural populace of Zimbabwe and help provide much needed trust and usage.

#### 4.3 Project Plan

****

#### 

#### 

#### 

#### 

#### 

#### 4.4 Conclusion

The existing documents highlight the existence of secure digital ID systems as having the potential to revolutionise the access to government services, the operations of her citizens, and their transparency enhancement in Zimbabwe. Enforcing the principles of Zero Trust and Privacy by Design will guarantee maximum security for the unique challenges of protecting the citizens of Zimbabwe. Additionally, while designing the system, mobile accessibility and offline usage will be introduced to designed system, thus promoting digital inclusion ensuring that all communities fully participate. Hence this project views the digital ID system being established in Zimbabwe not just as an improvement service but as a paradigm shaping all security and user-centered digital public services of the future.

#### References

* Banerjee, A., & Duflo, E. (2019). *Good Economics for Hard Times: Better Answers to Our Biggest Problems*. PublicAffairs.
* Deloitte. (2017). *Digital Identity: The essential guide*. Deloitte. Retrieved from
* Gelb, A., & Clark, J. (2013). *Identification for Development: The Biometrics Revolution*. Center for Global Development.
* Gelb, A., & Metz, A. (2018). *Identification Revolution: Can Digital ID be Harnessed for Development?* Center for Global Development.
* Heeks, R. (2006). *Implementing and Managing E-Government: An International Text*. SAGE Publications.
* Madise, Ü., & Martens, T. (2006). *E-government in Estonia: Best Practices and Perspectives*. Institute of Baltic Studies.
* Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Cengage Learning.
* World Bank. (2018). *The State of Identification Systems in Africa: A Synthesis of Country Assessments*. World Bank Group.
* Zwitter, A. (2014). Big Data ethics. *Big Data & Society*, 1(2), 1–6.
* Gutiérrez Zarza, Á. (2015). Processing and Protection of Personal Data in National Investigations and Criminal Proceedings.
* Kudakwashe Maguraushe, Adéle da Veiga and Nico Martins
* Journal: Information Security Journal: A Global Perspective, 2024, Page 1 DOI: 10.1080/19393555.2024.2329554