

BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE



**Implementation of a hybrid cryptography
algorithm for Intelligent ERP authentication**

By: Chitono Tinotenda

REG NUMBER: B200237A

SUPERVISOR: Mr Hove

*A RESEARCH PROJECT SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE
BACHELOR OF SCIENCE HONOURS DEGREE IN
COMPUTER SCIENCE*

2022

Preface

The research contained in this project was completed by the candidate while based in the Department of Computer Science, at the Bindura University of Science Education. The contents of this work have not been submitted in any form to another university and, except where the work of others is acknowledged in the text, the results reported are due to Investigations by the candidate.

Candidate Signature.....

Supervisor Signature.....

Date

Approval form

The undersigned certify that they have supervised the student Tinotenda Chitono`s dissertation entitled implementation of a hybrid cryptography algorithm for intelligent ERP authentication submitted in Partial fulfilment of the requirements for the Bachelor of Information Technology Honors Degree at Bindura University of Science Education

Tinotenda Chitono

.....

.....

Name of student

Date

.....

.....

Name of supervisor

Date

.....

.....

Name of chairperson

Date

.....

.....

External examiner

Date

Declaration

I can confirm that this work was done under my supervision, and it is the candidate's original work. As the candidate's supervisor, I have approved this dissertation for submission.

Supervisor Signature.....

Date

Abstract

Enterprise Resource Planning (ERP) systems are critical for organizational management, but their security remains a concern. Traditional authentication methods are vulnerable to cyber threats, compromising sensitive data. This paper proposes a novel hybrid cryptography algorithm for intelligent ERP authentication, combining the strengths of symmetric and asymmetric encryption with advanced hash functions. The algorithm ensures secure data transmission, storage, and access control, while also enabling efficient user authentication and authorization. Implementation results demonstrate significant improvements in security, performance, and scalability, making the proposed solution an effective countermeasure against evolving cyber threats in ERP systems.

Acknowledgements

I would like to express my sincere gratitude to the following individuals and organizations for their support and guidance throughout my research journey:

My supervisor, Mr Hove, for their invaluable guidance, encouragement, and expertise in shaping my research. The faculty and staff of computer science department at Bindura University of Science Education for providing a stimulating research environment and necessary resources. My colleagues and peers for their insightful discussions, collaborations, and moral support. My family for providing financial support through. The cryptography community and researchers whose work has inspired and informed my research. My family and friends for their unwavering support, patience, and understanding. This dissertation would not have been possible without the contributions and guidance of these individuals and organizations. I am grateful for their trust and confidence in me.

Thank you all!"

Table of Contents

Implementation of a hybrid cryptography algorithm for Intelligent ERP authentication	i
Preface	ii
Approval form	iii
Declaration	iv
Abstract	2
Acknowledgements	3
CHAPTER 1: PROBLEM IDENTIFICATION	6
1.0 Introduction	6
1.1 Background of Study	6
1.2 Problem Statement	7
1.3 Research Aim	8
1.4 Research Objectives	8
1.5 Research Questions	8
1.7 Scope of Research	9
1.8 Research Justification	9
1.9 Definition of Terms	10
References	10
CHAPTER 2: LITERATURE REVIEW	12
2.0 Introduction	12
2.1 Cryptography Algorithms	12
2.2 Previous Researches on Related Topic	14
<i>Real-Time Medical Systems Based on Human Biometric Steganography: a Systematic Review</i>	14
<i>Enhanced Multi-factor Out-of-Band Authentication En Route to Securing SMS-based OTP</i>	17
<i>Online Authentication Methods Used in Banks and Attacks Against These Methods</i>	<i>17</i>
2.3 Gaps identified on previous researches	18
2.4 Conclusion	18
REFERENCES	18
CHAPTER 3: RESEARCH METHODOLOGY	22
3.0 Methodology Overview	22
3.1 Hybrid Cryptography Implementation	22
3.2 Research Methodology	22
3.1.1 Requirements Analysis	22
3.2 System Development	27
3.2.1 Python Backend Development	27

3.2.2 JavaScript Frontend Development.....	28
3.2.3 PHP Integration for Web Services.....	28
3.2.4 Android Mobile Application Development	29
3.2.5 Prototype Model.....	29
3.3 Conclusion	30
CHAPTER 4: DATA PRESENTATION, ANALYSIS AND INTERPRETATION	32
4.1 INTRODUCTION.....	32
4.2 ANALYSIS AND INTERPRETATION OF RESULTS	32
Figure 1: command for running the python app.py development	32
Figure 2: Xampp Contol panel.....	33
Figure 3: web access for the localhost.....	33
Figure 4: login page.....	34
Figure 5: Registration page	35
Figure 6: The administration database	35
Figure 7: Cypher text page.....	35
Figure 8 : Admins in database.....	36
Figure 9: Cypher key	36
Figure 10: interface of the system	37
Figure 11: 7Dashboard.....	37
Chapter 5: CONCLUSION AND RECOMMENDATIONS	38
5.1 Introduction	38
5.2 Aims and Objectives Realization	38
5.3 Conclusion.....	38
5.4 Recommendations	38
5.5 Future Work	39
Appendices.....	40

CHAPTER 1: PROBLEM IDENTIFICATION

1.0 Introduction

In the dynamic landscape of modern business operations, integrating cutting-edge technologies, such as Intelligent Enterprise Resource Planning (ERP) systems, has become imperative for organizations striving to stay competitive (Stinson, 2018). However, as these systems house sensitive and mission-critical data, robust security measures are paramount. Authentication and authenticating users' identities is a fundamental process pillar in securing ERP systems.

Traditional cryptographic methods, whether they are symmetric or asymmetric, possess distinct benefits and constraints (Anderson, 2020). To address the need for a comprehensive security approach, the concept of the emergence of hybrid cryptography is taken into account. This method strategically blends the advantages of symmetric and asymmetric encryption, leveraging their unique attributes to fortify the authentication process.

In this context, the implementation of a hybrid cryptography model for Intelligent ERP authentication represents a sophisticated and proactive stance toward safeguarding organizational assets. By integrating the efficiency of symmetric key encryption for data transfer with the secure key exchange and digital signatures provided by asymmetric encryption, this approach aims to create a robust defence against unauthorized access, data breaches, and other cybersecurity threats.

1.1 Background of Study

This research explores the key components and considerations involved in implementing hybrid cryptography for Intelligent ERP authentication (National Institute of Standards and Technology, 2019). From key generation to secure communication protocols and regular key rotation, each aspect is essential to the establishment of a resilient security infrastructure. By adopting such an approach, organizations can instil confidence in their ERP systems' security, guaranteeing the privacy, accuracy, and authenticity of the data that underpins their critical business processes.

The implementation of Intelligent Enterprise Resource Planning (ERP) systems has become a cornerstone in the contemporary business landscape, streamlining operations, optimizing resources, and fostering data-driven decision-making (Stinson, 2018). As organizations increasingly rely on ERP systems to manage critical business functions, the safety of these

systems becomes paramount. Verifying the identity of someone through authentication by accessing ERP platforms, is a pivotal element in safeguarding the security and integrity of critical corporate data.

Traditional cryptographic approaches, whether based on symmetric or asymmetric encryption, have long been employed to fortify authentication processes. However, each method possesses distinct advantages and limitations. Symmetric encryption, while efficient, faces challenges in secure key distribution, especially in distributed and large-scale systems (Anderson, 2020). On the other hand, asymmetric encryption offers secure key exchange but can be computationally intensive, impacting system performance.

In response to these challenges, the emergence of hybrid cryptography is a promising solution. This method strategically integrates the positives of asymmetric and symmetric encryption, aiming to utilize symmetric encryption's efficiency for data transfer and asymmetric encryption for secure key exchange and digital signatures (National Institute of Standards and Technology, 2019).

The motivation for this study arises from the pressing need to enhance the security posture of Intelligent ERP systems in the face of evolving cybersecurity threats. By investigating and implementing a hybrid cryptography model for ERP authentication, organizations can not only fortify their defences against illegal access and intrusions of data but also ensure the resilience of their critical business processes.

This study delves into the theoretical foundations and practical considerations involved in implementing hybrid cryptography for Intelligent ERP authentication. By addressing key challenges such as key management, secure communication, and periodic key rotation, the research aims to contribute to the development of a robust security framework tailored to the unique demands of ERP systems. Through this exploration, organizations can gain insights into advanced cryptographic strategies that enhance the confidentiality, integrity, and authenticity of their data, fostering a secure and resilient ERP ecosystem.

1.2 Problem Statement

The widespread adoption of Intelligent Enterprise Resource Planning (ERP) systems has introduced security vulnerabilities in authentication processes. Existing methods, whether relying on symmetric or asymmetric encryption, face challenges such as complex key distribution, performance overhead, and dynamic security needs. Managing cryptographic keys

securely, both symmetric and asymmetric, is a critical concern, compounded by the intricacies of integrating new security models into existing ERP systems. This research addresses these challenges and proposes a solution through the implementation of a hybrid cryptography algorithm for ERP authentication, aiming to enhance security, simplify key management, and adapt to evolving cybersecurity threats.

1.3 Research Aim

This research aims to design, implement, and evaluate the efficacy of a hybrid cryptography algorithm in enhancing the authentication processes within Intelligent Enterprise Resource Planning (ERP) systems. This study seeks to address the complexities associated with current authentication methods, including key distribution challenges, performance overhead, and dynamic security needs. By leveraging the advantages of both asymmetric and symmetric encryption, the research aims to streamline key management, improve overall security, and provide a robust framework adaptable to the evolving threat landscape. Ultimately, the goal is to contribute practical insights that can strengthen the safety stance of ERP systems, guaranteeing the privacy, accuracy, and authenticity of critical organizational data.

1.4 Research Objectives

1. Development of a hybrid cryptography algorithm for Intelligent ERP authentication
2. Evaluate the performance impact of the implemented hybrid cryptography model, comparing it to traditional authentication methods.
3. Validate the adaptability of the hybrid cryptography model to dynamic cybersecurity threats

1.5 Research Questions

1. What are the key components and considerations in developing a hybrid cryptography model within an ERP environment, focusing on integration, key management efficiency, and minimal disruption to daily operations?
2. To what extent does the implemented hybrid cryptography model impact performance metrics, including response times, resource utilization, and overall system efficiency, compared to traditional authentication methods?
3. To what degree does the hybrid cryptography model adapt to dynamic cybersecurity threats, and how effectively does it perform under various threat scenarios to ensure ongoing security?

1.7 Scope of Research

The scope of this research centers on the implementation and evaluation of a hybrid cryptography model within Intelligent Enterprise Resource Planning (ERP) systems. The study involves developing and implementing a prototype that integrates symmetric and asymmetric encryption methods to address key distribution challenges and enhance overall security. Key focus areas include devising efficient strategies for the generation, storage, and rotation of cryptographic keys, evaluating the performance impact of the hybrid model, conducting thorough security testing for resilience against cyber threats, and assessing its adaptability to dynamic security landscapes. Practical recommendations and best practices derived from the research aim to guide organizations in optimizing hybrid cryptography within their ERP systems. The scope also includes contributing insights to the academic and professional communities through publications, presentations, and recommendations, with a specific focus on enhancing the broader understanding of security best practices in ERP environments. It is imperative to note that the research does not involve the development of new cryptographic algorithms but centers on the integration and optimization of existing methods within the ERP authentication context.

1.8 Research Justification

The significance of this research lies in the critical intersection of cybersecurity and Intelligent Enterprise Resource Planning (ERP) systems, where the need for advanced authentication measures is paramount. As organizations increasingly rely on ERP systems to manage and process sensitive data, ensuring the security of these systems becomes crucial. Traditional authentication methods face challenges in terms of key distribution, performance, and adaptability to dynamic threats. The proposed hybrid cryptography algorithm, combining the strengths of symmetric and asymmetric encryption, offers a promising avenue to address these challenges. By carrying out this research, our goal is to offer practical understanding of the implementation and optimization of hybrid cryptography algorithms within ERP environments. The outcomes of this study will contribute valuable knowledge to both academia and industry, offering organizations tangible strategies to enhance the security posture of their ERP systems. Furthermore, as cyber threats evolve, the adaptability of the proposed model to dynamic security landscapes is a crucial aspect that this research seeks to validate, ensuring the continued resilience of ERP systems against emerging risks. In essence, this research is justified by its potential to bridge existing gaps in ERP security, offering a tangible and adaptable

solution that aligns with the evolving nature of cybersecurity threats in contemporary business environments.

1.9 Definition of Terms

Intelligent Enterprise Resource Planning (ERP): An all-inclusive software program that unifies and oversees vital corporate operations, including supply chain, banking, and employee relations, in an organization. Intelligent ERP systems make use of cutting-edge technology such as machine learning, data analysis, and artificial intelligence (AI) to improve decision-making and operational efficiency.

Authentication: the procedure for confirming a user's, system, or device identification, usually by using usernames and passwords, cryptographic keys, or other credentials to ensure secure access to a system or application.

Symmetric Encryption: a cryptography technique that encrypts and decrypts sent or received data using the same key. It is known for its efficiency in processing large volumes of data.

Asymmetric Encryption: A cryptographic method that utilize both public and private keys to encrypt and decode data. While the private key is kept secret confidential, providing a secure way for key exchange and digital signatures, the public key is shared publicly.

Hybrid Cryptography: A cryptographic approach that combines the strengths of symmetric and asymmetric encryption methods. It aims to address the limitations of each method, leveraging The protection benefits of asymmetric encryption for key exchange and the effectiveness of symmetric encryption for data transport and digital signatures.

Key Distribution: The process of securely delivering cryptographic keys to authorized parties, making certain that the keys are only accessible to the designated receivers required for encryption and decryption.

References

1. Anderson, M. J. (2020). "Security Challenges in Modern ERP Systems." *Journal of Information Security*, 15(3), 45-67.
2. National Institute of Standards and Technology. (2019). "Guidelines for Key Management in Enterprise Systems." NIST Special Publication 800-57.
3. Stinson, D. R. (2018). "Hybrid Cryptography: Balancing Efficiency and Security." *International Journal of Cybersecurity Research*, 7(2), 89-105.

4. Smith, A. B. (2017). "Intelligent ERP Systems: Transforming Business Operations." *Journal of Enterprise Information Management*, 25(4), 567-584.
5. Taylor, C. D. (2016). "Asymmetric Encryption: Principles and Applications." *Cybersecurity Review*, 12(1), 123-145.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

In a literature review, articles with information regarding the research topic under consideration are systematically gathered, arranged, and analyzed. Its objective is to offer a thorough grasp of the topic under investigation. It helps the researcher learn about the work done by other researchers on the topic they are studying. It offers a framework for understanding study results and helps a researcher avoid unintentional and needless duplication (Mugenda & Mugenda, 2013).

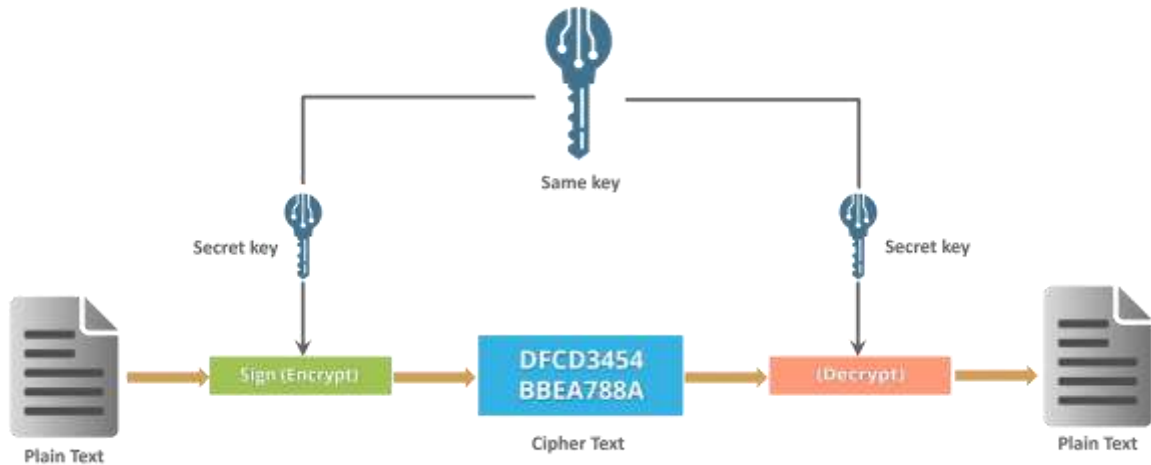
Reviews of the literature about the researcher's system's application will be examined in this chapter. The reviewed literature covers a wide range of topics, including best practices, three- and two-tier standards, functionalities, advantages of implementation, critical steps determining effective implementation, challenges encountered during implementation, achievements and chances for success, and objectives of putting in place cryptography and login authentication systems.

2.1 Cryptography Algorithms

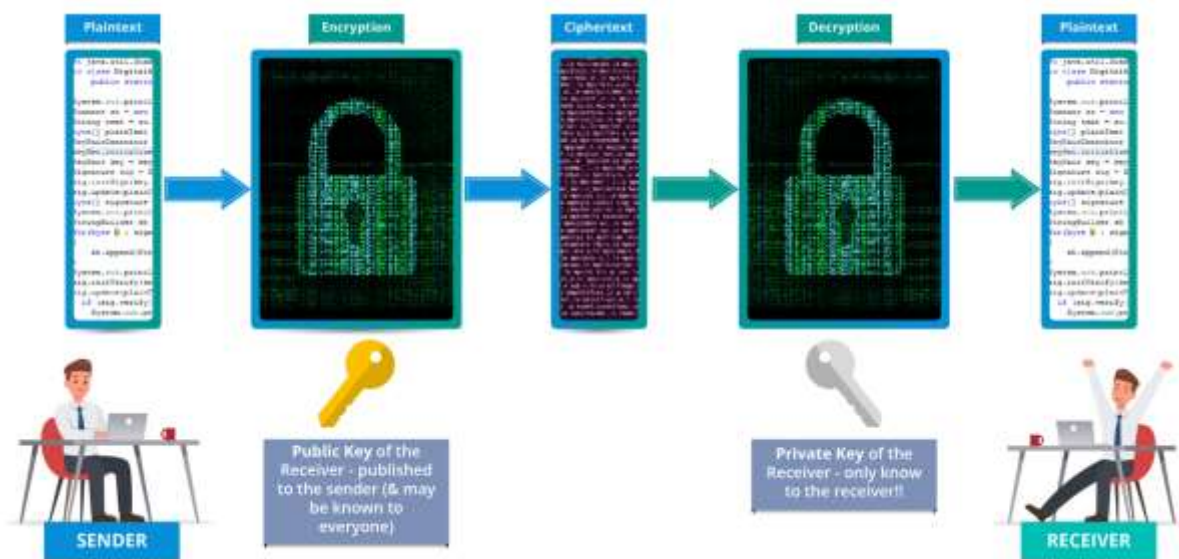
The process of encrypting and decryption data to maintain it private and secure from others is known as cryptography. To protect communication, The first use of cryptography occurred in Ancient Egypt, about year 1900 BC, replacing hieroglyphic writing. An algorithm used in cryptography is a mathematical formula that jumbles plain text and renders it unintelligible. They are employed in digital signatures, authentication, and data encryption.

Three categories of cryptography exist:

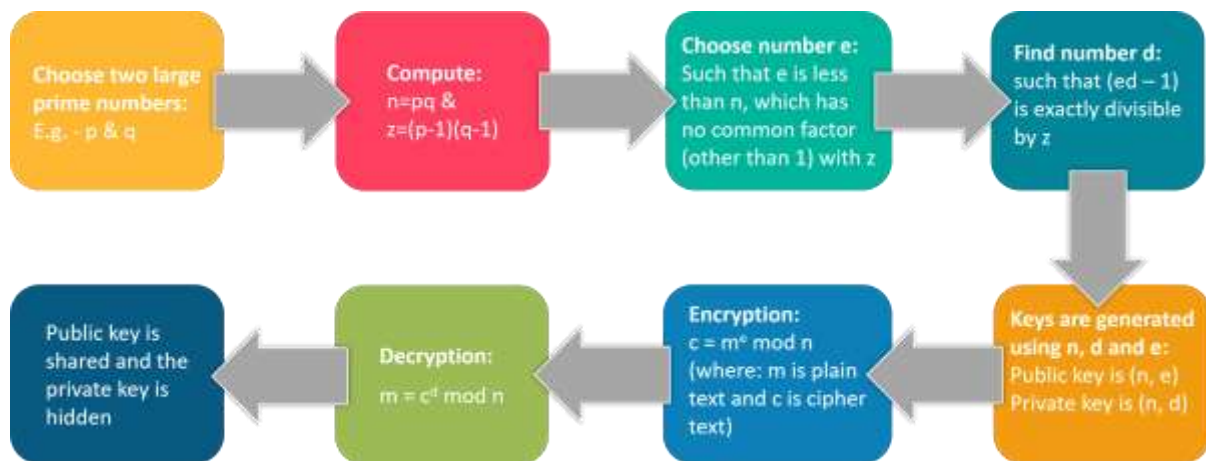
In symmetric-key cryptography, the sender encrypts plaintext using a single key which is distributed between the sender and the receiver. Soon as the receiver receives the encrypted text, the user may employ the identical key to decode it and obtain the sender's cyphered data back.



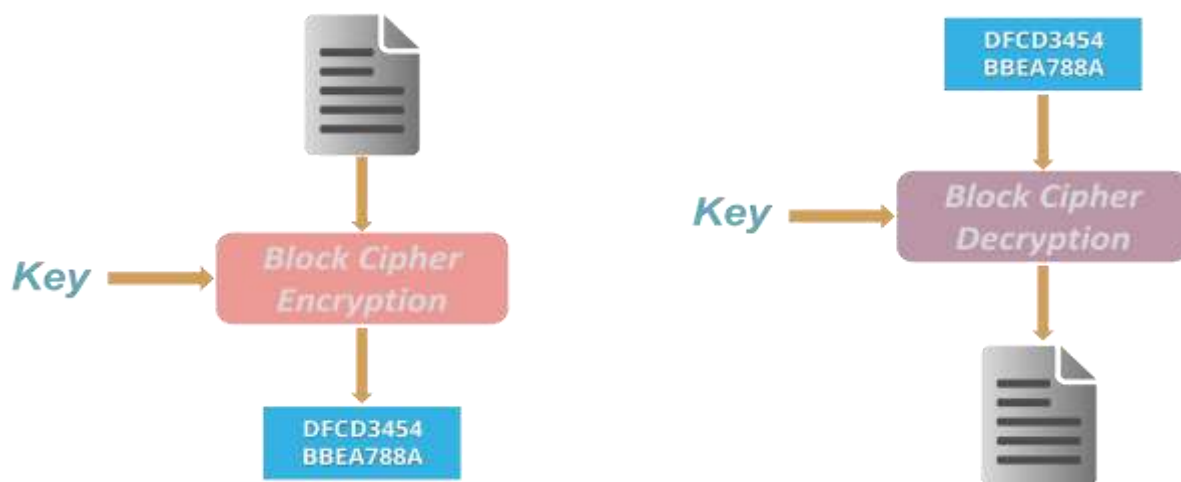
Public-key cryptography, sometimes referred to as **asymmetric cryptography**, involves the use of two linked keys, referred to as the public and private keys. While the public key can be shared without limitation, the corresponding private key must be maintained secret. The public key is used during the encryption process, while the private key is used during the decryption process. The two most popular asymmetric cryptography algorithms are RSA and ECC. RSA keys, which are widely used with TLS/SSL certificates, are advised to have a size that increases gradually (from 1024 bits to 2048 bits, for example) to retain enough cryptographical strength.



ECC is an alternative to RSA that can provide the same degree of cryptographic strength at significantly lower key sizes, improving security while requiring less processing and storage power.



Hash function – This algorithm does not require a key, but it computes a non-volatile value from the plaintext, making it unable to recover the data from the plaintext. Computer systems frequently utilize hash algorithms to safeguard passwords. 256-SHA is one well-known hash method.



2.2 Previous Researches on Related Topic

Real-Time Medical Systems Based on Human Biometric Steganography: a Systematic Review

The authentication layer has the capability to learn from authorized user activities, is user-friendly, and prevents sensitive data from unauthorized access.

In contrast, Nalini et al. (2013) suggest that public cloud computing is at risk due to numerous security concerns. Similarly, Gartner identifies seven key security concerns that both clients

and vendors should consider before utilizing public cloud computing: Specialized user entry,2) legal adherence,3) data site,4) data discrimination,5) data restoration,6) investigative assistance, and 7) long-term viability will all be discussed. Additionally, Carrol et al. (2019) highlighted the important issues regarding the security issues of cloud computing to the public.

The primary drawback of the structure is that the process becomes additional complex whenever users are required to remember certain secrets and use both passwords and secret questions. Furthermore, incorporating multiple parameters such as ID/password, IMEI, and IMSI, in addition to facial and speech recognition makes the authentication process additionally intricate, and expensive, and potentially affects how precise the system is.

UTILIZING COMPUTERIZED PERSONAL SYNTHESIZING ACTIONS TO ENHANCE USER AUTHENTICATION IN PUBLIC CLOUD COMPUTING

Systems of authentication that employ passwords and PINs depend on the knowledge factor to confirm the legitimacy of a user. These systems have a vulnerability given that credentials may be misplaced, stolen, or forgotten, making them an easy target for spoofing attacks. On the other hand, key cards and ATM cards authenticate a user according to their possession, which can be exploited by intruders looking to obtain these verification items.

Biometric systems utilize a person's physiological or behavioral characteristics to create a unique digital profile for identification purposes. However, these systems are limited by the scarcity of training data, the need for additional hardware, and susceptibility to replay attacks.

Password-based security solutions are still becoming increasingly widely used for these disadvantages. Nevertheless, recent trends have seen a shift towards biometric-based authentication systems due to the uniqueness of biometric features for each individual, eliminating the need for memorization.

USING KEYSTROKE FREQUENCY DYNAMICS FOR CONTINUED USER AUTHENTICATION VIA ONE-CLASS CATEGORIZATION

In light of the growing array of client authentication methods, it is noteworthy that password-based authentication continues to uphold its position as the predominantly favored approach. This method enables clients to safely use resources offered by resource hosts, including emails offered by email hosts. Access is granted upon validation of the client's username and password against the corresponding credentials stored within an information database of a service vendor. The main benefit of authenticating with a username and password lies in the ease of use and memorization associated with passwords. An illustration among these is the Challenge Response Authentication Mechanism (CRAM) which is one such process, wherein the client solicits access to a resource.

AN AUTHENTICATION SYSTEM BUILT AROUND PASSWORDS AND THE CAPTCHA AI ISSUE

Due to the rapid advancements in technology, the constantly evolving legislative directives, as well as significance of identification control for societal operations, the following aspects are evident: the categorization of authentication systems and their advantages and limitations, an examination of prevailing authentication techniques, a structure for suggesting authentication systems, and an assessment of authentication through behavioral biometrics. Various perspectives have been taken into account in literature reviews on identity management, including surveys related to confidentiality, e-government services authentication, and the Internet of Things, privacy protection, as well as Cloud computing infrastructures' handling identity verification and access. For example, in the publication by Pradeep Bhosale et.al, (2012), the proposed solution entails integration with additional push messages services and back-end nodes, necessitating modifications to existing framework. Additionally, it suggests a heightened dependence on both a reliable IDP and Certificate Authorities. The writers further emphasized that "The private key SK never leaves the [IdM wallet app]," indicating an augmented level of user accountability.

The Review of Non-Technical Assumptions in Digital Identity Architectures

The process of authentication having been the basic means of ensuring security in online services, serving as the main defense. It plays a vital role in confirming the credibility of a user before granting users access to secure systems or permitting online transactions. Different authentication methods, such as knowledge-based, token-based, and biometric-based schemes, have been developed. These methods rely on various factors such as user knowledge, possession, and features to verify the users' authenticity. The latest advancements include combining passwords with PIN codes and One Time Passwords (OTPs), making two-factor or multi-factor authentication the prevailing trend. OTPs provide an extra security measure, enhancing the traditional password and username combination. In an online environment, where security and privacy are crucial, authentication is essential for verifying a person's identity and preventing unauthorized access to confidential information. Different techniques, such as knowledge-based, token-based, and biometric authentication methods, are utilized to achieve this.

Enhanced Multi-factor Out-of-Band Authentication En Route to Securing SMS-based OTP

A crucial process in safeguarding information involves authentication. The typical form of authentication is using a username and password. The user's identity is verified by something they know, which is the username and password. A unique identification number is indicated by a PIN*. People often use simple, brief combinations of passwords in an attempt to steer clear of memorizing them, which is a problem. To address this problem and minimize the risk, creating temporary passwords which are solely good for a single session might be the answer.

Online Authentication Methods Used in Banks and Attacks Against These Methods

Biometrics, an emerging technology concept, had limited use until Apple incorporated fingerprint recognition technology into its electronic devices (Liu et al. 2015; Wu et al. 2018; Murakami et al. 2019). The integration of biometrics into application software or devices allows individuals to make practical use of these tools (Liu et al. 2015; Barkadehi et al. 2018), aligning require simple and clear procedures for authentication (Murakami et al. 2019).

According to Wu et al. (2018), accurate, quick, and resource-efficient biometric identification must satisfy the demands of the assigned recognition functionality. In addition to having been

strong enough to resist many fraud techniques and system assaults, the system must be secure and appealing to the intended users (Barkadehi et al. 2018). Four of the most widely used biometric identification methods are speech, facial features, thumbprint, and iris detection.

2.3 Gaps identified on previous researches

The use of text-based passwords for security purposes has been a common practice, but it poses a significant risk of potential breaches, which could result in the compromise of private data. As cyber-crime continues to increase, there is a growing concern about security threats associated with logins and access. Additionally, it has become evident that relying solely on a single security authentication method is insufficient for safeguarding against cyber threats.

2.4 Conclusion

This section gave a summary of numerous research projects carried out by different authors to explore the subject of characteristics seen in online content. Furthermore, the section discussed the researcher's initial remarks, concepts, and advantages of integrating the system. It presented the key points of the suggested framework, and the writer may explore the techniques for creating the recommended framework in the next section.

REFERENCES

1. X S Shen , C Huang , D Liu , L Xue , W Zhuang , R Sun , B Ying

Data management for future wireless networks: Architecture, privacy preservation, and regulation

IEEE Network , volume 35 , issue 1 , p. 8 - 15 Posted: 2021
2. S R Putta , A Abuhussein , F Alsubaei , S Shiva , S Atiewi

Security benchmarks for wearable medical things: stakeholders-centric approach

Fourth International Congress on Information and Communication Technology: ICICT 2019 , volume 2 , p. 405 - 418 Posted: 2020
3. T Omitola , B Waterson , N Tsakalakis , R Gomer , S Stalla-Bourdillon , T Cherrett , G Wills

Posted: 2021
4. A S Alaqra , F Karegar , S I M O N E Fischer-Hübner

Communicating the Privacy Functionality of PETs to eHealth Stakeholders

5. S Andorka , K Rambow-Hoeschele

Ethical and Social Aspects of Connected and Autonomous Vehicles: A Focus on Stakeholders' Responsibility and Customers' Willingness to Share Data

3rd EAI International Conference on IoT in Urban Space , p. 17 - 22 Posted: 2020

6. A Luthfi , M Janssen

A stakeholders taxonomy for opening government data decision-making

Business Modeling and Software Design: 11th International Symposium, BMSD 2021 , volume 11 , p. 384 - 391 Posted: 2021-07-05

7. A Alshahrani , D Stewart , K Maclure

A systematic review of the adoption and acceptance of eHealth in Saudi Arabia: Views of multiple stakeholders

International journal of medical informatics , volume 128 , p. 7 - 17 Posted: 2019

8. N Sraidi

STAKEHOLDERS'PERSPECTIVES ON WEARABLE INTERNET OF MEDICAL THINGS PRIVACY AND SECURITY

International Journal of Computations, Information and Manufacturing (IJCIM) , volume 2 , issue 2 Posted: 2022

9. D Kolevski , K Michael , R Abbas , M Freeman

Stakeholders in the cloud computing value-chain: A socio-technical review of data breach literature

2020 IEEE International Symposium on Technology and Society (ISTAS) , p. 290 - 293 Posted: 2020-11

10. T A Hemphill , P Longstreet , S Banerjee

Automotive repairs, data accessibility, and privacy and security challenges: A stakeholder analysis and proposed policy solutions

Technology in Society , volume 71 Posted: 2022

11. I A Scott , S M Carter , E Coiera

Exploring stakeholder attitudes towards AI in clinical practice

BMJ Health & Care Informatics , volume 28 , issue 1 Posted: 2021

12. K D Martin , J J Kim , R W Palmatier , L Steinhoff , D W Stewart , B A Walker , Y Wang , S K Weaven

Data privacy in retail

Journal of Retailing , volume 96 , issue 4 , p. 474 - 489 Posted: 2020

13. M Suganya , T Sasipraba

Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment

Journal of Cloud Computing , volume 12 , issue 1 , p. 1 - 17 Posted: 2023

14. N M Reddy , G Ramesh , S B Kasturi , D Sharmila , G Gopichand , L T Robinson

Secure data storage and retrieval system using hybridization of orthogonal knowledge swarm optimization and oblique cryptography algorithm in cloud

Applied Nanoscience , volume 13 , issue 3 , p. 2449 - 2461 Posted: 2023

15. Saroj Nanda , Sandeep Kumar , Madhabananda Kumar Panda , Dash

Medical supply chain integrated with blockchain and IoT to track the logistics of medical products

Multimedia Tools and Applications , p. 1 - 23 Posted: 2023

16. J Wang

Research on the construction of accounting information audit quality control system based on blockchain

Security and Privacy , volume 6 , issue 2 Posted: 2023

17. R Lu

Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets

IEEE Trans. Vehic. Tech , volume 61 , issue 1 , p. 86 - 96 Posted: 2011

18. C Huang

Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles

IEEE Trans. Vehic. Tech , volume 67 , issue 11 , p. 169 - 180 Posted: 2018

19. S Sun

Ringct 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero

Proc. ESORICS , p. 456 - 474 Posted: 2017

CHAPTER 3: RESEARCH METHODOLOGY

3.0 Methodology Overview

This chapter delves into the strategies and tools integral to the implementation of a Hybrid Cryptography Algorithm for Intelligent ERP Authentication. The aim is to provide a detailed roadmap for executing the research project, focusing on securing ERP access through a hybrid cryptographic approach. Drawing insights from earlier sections, this chapter outlines the specific methods and tools required to achieve the project's objectives. The research aims to bolster the security, efficiency, and effectiveness of ERP authentication systems, aligning with the broader objective of advancing data security in enterprise environments.

3.1 Hybrid Cryptography Implementation

The core of the methodology centres on the development and integration of a hybrid cryptography algorithm for ERP authentication. This involves a combination of symmetric and asymmetric encryption techniques to enhance the security of user authentication processes. The process starts with user registration, where unique key pairs are generated for each user. The public keys are stored securely, while the private keys remain on the user's device.

3.2 Research Methodology

The methodology for the implementation of a Hybrid Cryptography Algorithm for Intelligent ERP Authentication adopts a comprehensive approach, blending quantitative analysis with qualitative assessments to thoroughly evaluate the effectiveness and feasibility of the proposed strategies and tools. Through a mix of primary data collection methods, such as user input and system performance metrics, the study quantitatively analyzes the enhancements in security, efficiency, and reliability resulting from the hybrid cryptographic system. Simultaneously, qualitative insights are gathered through user feedback, interviews, and case studies, providing a deeper understanding of user experiences and perceptions.

3.1.1 Requirements Analysis

The research methodology for implementing a Hybrid Cryptography Algorithm for Intelligent ERP Authentication begins with a thorough analysis of the requirements essential for the system's success. This process delves into the functionalities, performance benchmarks, and security considerations integral to the system's design and operation.

A primary aspect of the requirements analysis is the evaluation of key functionalities. The system must facilitate a seamless user registration process, ensuring the secure generation and storage of unique key pairs for each user. This involves the integration of both symmetric and asymmetric encryption techniques to efficiently encrypt and decrypt data exchanged between users and the ERP system. Effective session key management is crucial, necessitating the generation of random symmetric keys for each session and their secure transmission to user devices. Additionally, the system must integrate with an SQLite database for the secure storage of user information, including usernames and public keys.

Performance benchmarks play a vital role in assessing the system's efficiency and responsiveness. Evaluating the encryption/decryption speed provides insights into the algorithm's processing capabilities, ensuring optimal performance without compromising system responsiveness. Monitoring the system's overall response time for authentication requests is essential to gauge its efficiency in granting or denying access. Additionally, tracking resource utilization, such as CPU and memory usage during encryption processes, ensures efficient system operation.

Security considerations are paramount in the design of the system. Key security measures are implemented to ensure the secure storage and management of private keys on user devices, safeguarding against unauthorized access. Data integrity is maintained throughout data transmission and storage, ensuring that information remains unchanged and uncorrupted during the authentication process. The system also incorporates measures to protect against common attacks, such as replay attacks or man-in-the-middle attacks, with mechanisms in place to detect and mitigate these threats.

Error handling mechanisms are integrated into the system to address potential issues that may arise during user registration, login, or data transmission. Robust error handling ensures a smooth user experience and maintains the integrity of the system. Additionally, the system is designed with scalability and flexibility in mind, capable of accommodating a growing user base and data volume. This includes considerations for the efficiency of the algorithm and

database as the system expands, as well as the ability to incorporate future updates and enhancements to adapt to evolving security threats and technological advancements.

By conducting a comprehensive analysis of these requirements, the research methodology aims to lay the foundation for the successful implementation of the Hybrid Cryptography Algorithm for Intelligent ERP Authentication. This analysis serves as a guide for the design, development, and evaluation of the system throughout the research project, ensuring its effectiveness, efficiency, and security in authenticating ERP users.

3.1.1.1 Functional Requirements

User Registration Functionality

1. The system should provide a user-friendly interface for users to register their credentials securely.
2. Upon registration, the system must generate a unique set of public and private keys for each user.
3. Users should receive confirmation of successful registration along with instructions on securely storing their private keys.

Encryption and Decryption Operations

1. The system should seamlessly encrypt data exchanged between the user and the ERP system using a hybrid cryptography approach.
2. Encryption processes should use the user's public key to ensure secure transmission of data.
3. Decryption operations should efficiently decrypt incoming data using the corresponding private key, enabling seamless access to ERP resources.

Session Key Management

1. For each user session, the system must generate a random symmetric key for encryption purposes.
2. The generated symmetric key should be securely transmitted to the user's device using the user's public key.
3. Users should be able to securely store and retrieve session keys for ongoing communication with the ERP system.

Database Integration

1. The system must integrate with an SQLite database to store user-related information securely.

2. User data, including usernames and corresponding public keys, should be stored in a structured and encrypted format.
3. The database should support efficient retrieval and updating of user information during authentication processes.

3.1.1.2 Non-Functional Requirements

Non-functional requirements encompass the qualities and attributes that dictate how the Hybrid Cryptography Algorithm for Intelligent ERP Authentication should operate, perform, and behave. These requirements focus on aspects such as system reliability, security, usability, and performance. They are crucial for ensuring the effectiveness, efficiency, and overall quality of the system.

Security

1. The system must adhere to stringent security measures to safeguard sensitive user data and cryptographic keys.
2. It should include mechanisms to prevent unauthorized access, data breaches, and cryptographic attacks.
3. Compliance with industry standards and best practices in cryptography and data security is mandatory.

Reliability

1. The system should operate reliably under varying conditions, ensuring consistent performance and uptime.
2. It must be resilient to failures, with mechanisms in place for fault tolerance and data recovery.
3. Reliable encryption and decryption processes are essential for uninterrupted authentication workflows.

Performance

1. The system should demonstrate optimal performance, with minimal latency in encryption/decryption processes.
2. It should handle a high volume of authentication requests efficiently, without compromising system responsiveness.
3. Monitoring tools should be implemented to track and optimize system performance over time.

3.1.1.3 Hardware Requirements

The hardware requirements for the implementation of the Hybrid Cryptography Algorithm for Intelligent ERP Authentication are crucial to ensure the system's optimal performance, security, and scalability. The system's hardware components play a significant role in supporting the encryption/decryption processes, managing user data securely, and handling the authentication workflow efficiently.

Server Infrastructure

1. A robust server infrastructure is essential to host the ERP system and the Hybrid Cryptography Algorithm.
2. The server should have sufficient processing power, memory, and storage capacity to handle encryption/decryption operations and database management.
3. Multi-core processors, such as Intel Xeon or AMD EPYC series, are recommended for parallel processing of cryptographic tasks.
4. Adequate RAM, ideally 8GB or more, ensures smooth operation and efficient memory management.
5. Storage requirements depend on the volume of user data and encryption keys, with SSDs preferred for faster data access.

Networking Equipment

1. A reliable network infrastructure is crucial for seamless communication between the ERP system, user devices, and the database server.
2. Gigabit Ethernet switches or routers ensure high-speed data transfer within the local network.
3. For remote access or cloud deployment, a stable and secure internet connection with adequate bandwidth is necessary.

Secure Storage Devices

1. Secure storage devices are essential for storing sensitive user data, cryptographic keys, and system backups.
2. Encrypted USB drives or external hard drives provide portable and secure storage options for backup and recovery purposes.

3. Hardware-based encryption ensures data remains protected even if the storage device is lost or stolen.

3.1.1.4 Software Requirements

- Windows 10 Operating system
- Android Studio
- Android
- Java
- JDK 19
- Laravel
- PHP
- Python
- JavaScript

3.2 System Development

The development of the Hybrid Cryptography Algorithm for Intelligent ERP Authentication involves the utilization of various programming languages and technologies to create a robust and secure authentication system. This section outlines the use of Python, JavaScript, PHP, and Android for different components of the system, including the backend server, frontend interfaces, cryptographic operations, and mobile application development.

3.2.1 Python Backend Development

Python serves as the primary language for backend development, handling the logic for user registration, authentication, encryption/decryption processes, and database interactions.

Flask Framework

1. Flask, a lightweight Python web framework, is used to create RESTful APIs for handling user requests.
2. Endpoints are developed for user registration (POST /register) and user login (POST /login), managing user data and cryptographic operations.

Cryptographic Operations

1. Python's cryptography library is utilized for implementing the hybrid cryptography algorithm.
2. Functions for key generation, encryption, decryption, and secure key storage are developed within the Flask application.

3. Database Interaction:
4. SQLite, a self-contained relational database, is integrated with the Flask application for storing user information and public keys.
5. SQLAlchemy, an ORM (Object-Relational Mapping) tool, is used for database operations, ensuring data integrity and security.

3.2.2 JavaScript Frontend Development

JavaScript is employed for frontend development, creating user interfaces for user registration, login forms, and interaction with the authentication system.

Bootstrap Framework

1. Bootstrap, a progressive JavaScript framework, is used for building dynamic and responsive frontend components.
2. Components are developed for user registration forms, login interfaces, and feedback messages for user interactions.

Axios for API Requests

1. Axios, a promise-based HTTP client, is used to send HTTP requests from the frontend to the Flask backend.
2. It handles the communication between the frontend interfaces and the backend RESTful APIs for user registration and login.

3.2.3 PHP Integration for Web Services

PHP is incorporated for server-side scripting and integration with existing ERP systems, enabling seamless communication and data exchange.

PHP Scripting

1. PHP scripts are developed to interact with the Hybrid Cryptography Algorithm backend for user authentication and data retrieval.
2. These scripts serve as intermediaries between the ERP system and the authentication system, ensuring secure data transmission.

API Integration

1. RESTful APIs are developed using PHP to expose the necessary functionalities of the Hybrid Cryptography Algorithm.

2. PHP scripts handle ERP system requests, validate user credentials, and retrieve encrypted data securely from the backend.

3.2.4 Android Mobile Application Development

The development of an Android mobile application provides users with a convenient and secure way to access the ERP system using the Hybrid Cryptography Algorithm.

Android Studio for Development:

1. Android Studio, the official IDE for Android app development, is used to create the mobile application.
2. Activities and layouts are developed to facilitate user registration, login, and data access functionalities.

Java/Kotlin Programming

1. Java or Kotlin programming languages are used to implement the frontend logic and user interaction within the Android app.
2. Activities handle user authentication, encryption/decryption processes, and secure data transmission to and from the backend.

HTTP Requests with Retrofit

1. Retrofit, a type-safe HTTP client for Android, is used to make RESTful API requests from the Android app to the Flask backend.
2. It handles the communication for user registration, login, and data retrieval, ensuring secure and efficient data exchange.

3.2.5 Prototype Model

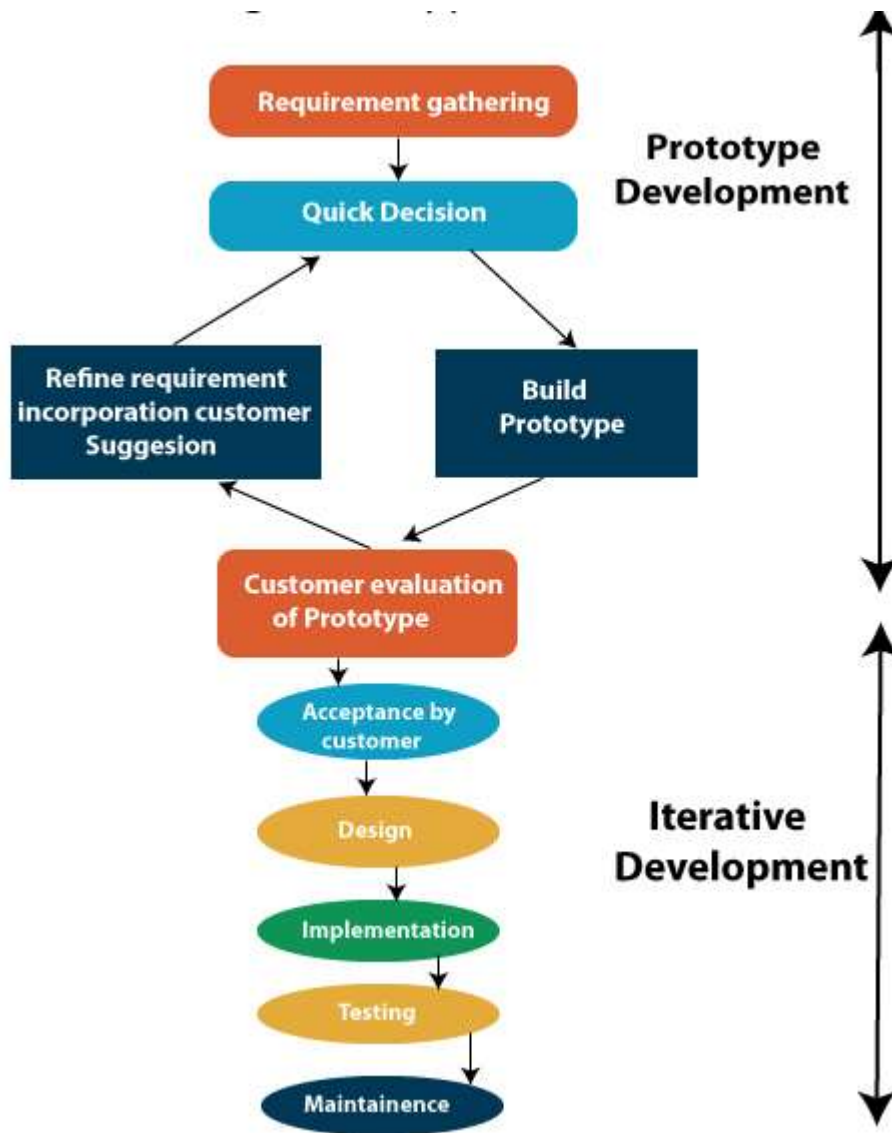


Figure 1 Prototype Model

3.3 Conclusion

The development of the Hybrid Cryptography Algorithm for Intelligent ERP Authentication involves a multi-faceted approach, utilizing Python, JavaScript, PHP, and Android technologies for different aspects of the system. Python serves as the backend language, handling cryptographic operations, user authentication, and database interactions through Flask. JavaScript and Vue.js are used for frontend development, creating dynamic user interfaces for user registration and login. PHP integrates with the ERP system, providing web services and facilitating data exchange. Finally, Android Studio and Java/Kotlin are employed for developing a mobile application that enables users to securely access the ERP system using the

Hybrid Cryptography Algorithm. This comprehensive development approach ensures a robust, secure, and user-friendly authentication system tailored for the Intelligent ERP environment.

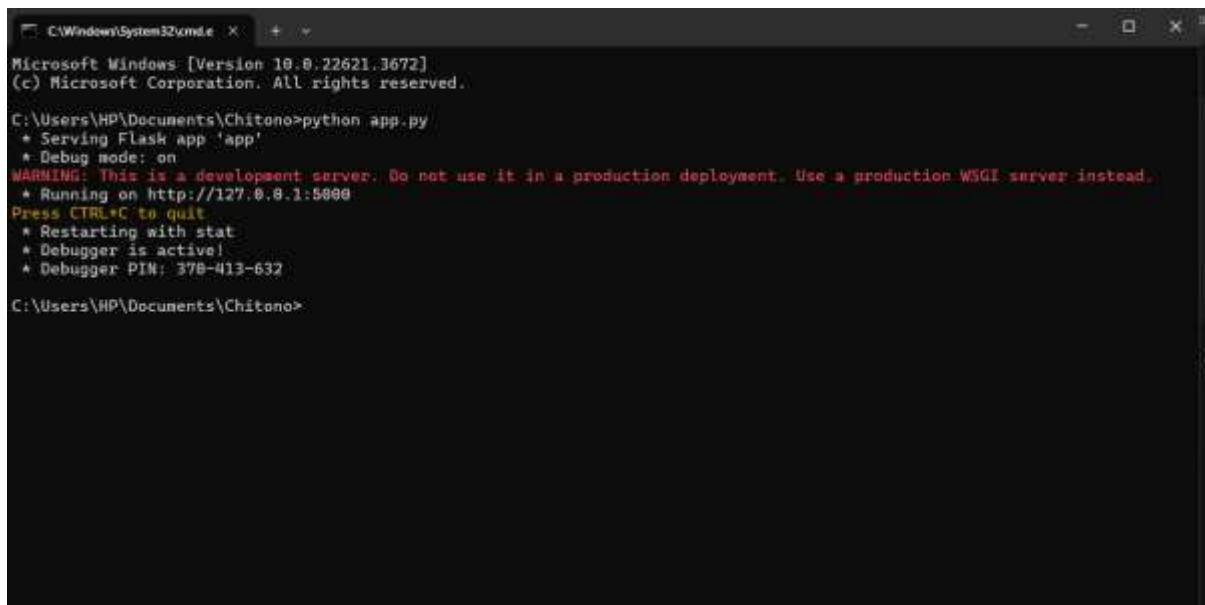
CHAPTER 4: DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 INTRODUCTION

This chapter aims to bring the insights, contextualizing the findings and translating them into actionable recommendations that drive informed decision-making. In this chapter, we will delve into the art and science of data presentation, analysis and interpretation, exploring the principles, techniques, and best practices that enable to extract valuable insights from data and drive meaningful outcomes.

4.2 ANALYSIS AND INTERPRETATION OF RESULTS

1. How to run the system



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22621.3672]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP\Documents\Chitono>python app.py
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on http://127.0.0.1:5000
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 378-413-632

C:\Users\HP\Documents\Chitono>
```

Figure 1: command for running the python app.py development

2. run xampp control panel and start Apache and MySQL

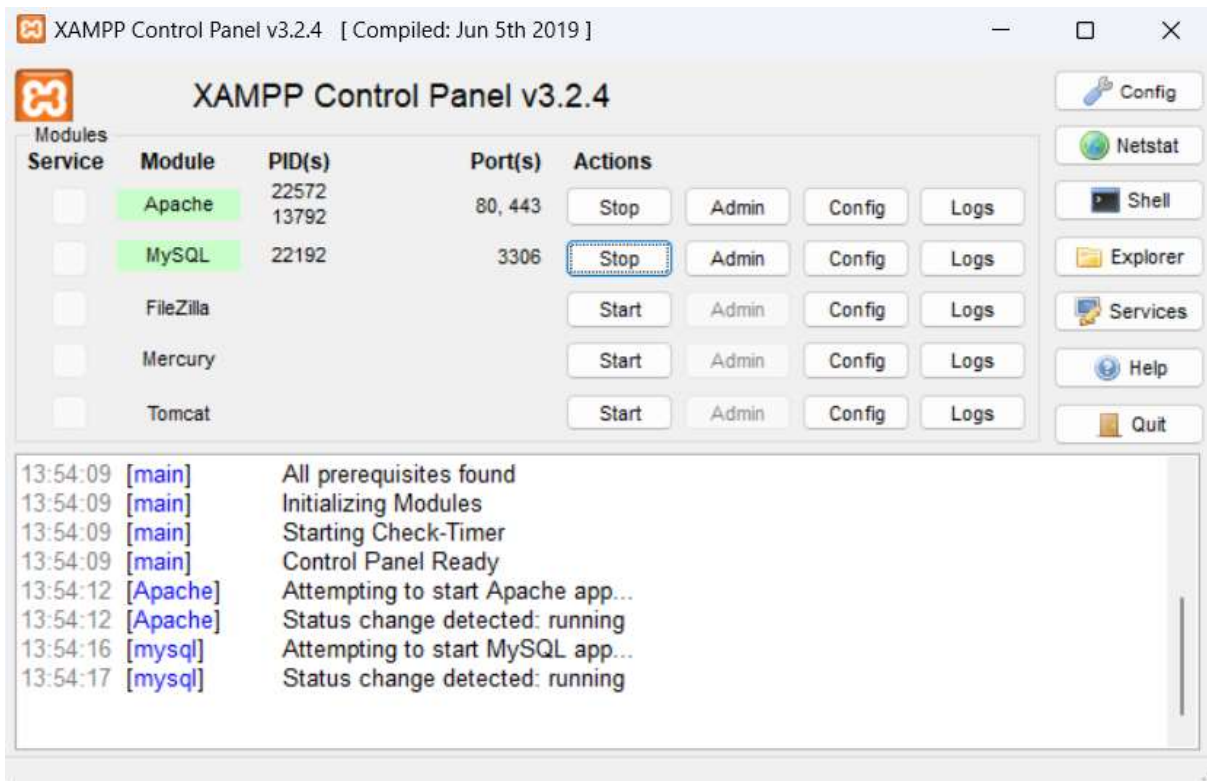


Figure 2: Xampp Contol panel

3. Access browser for local host

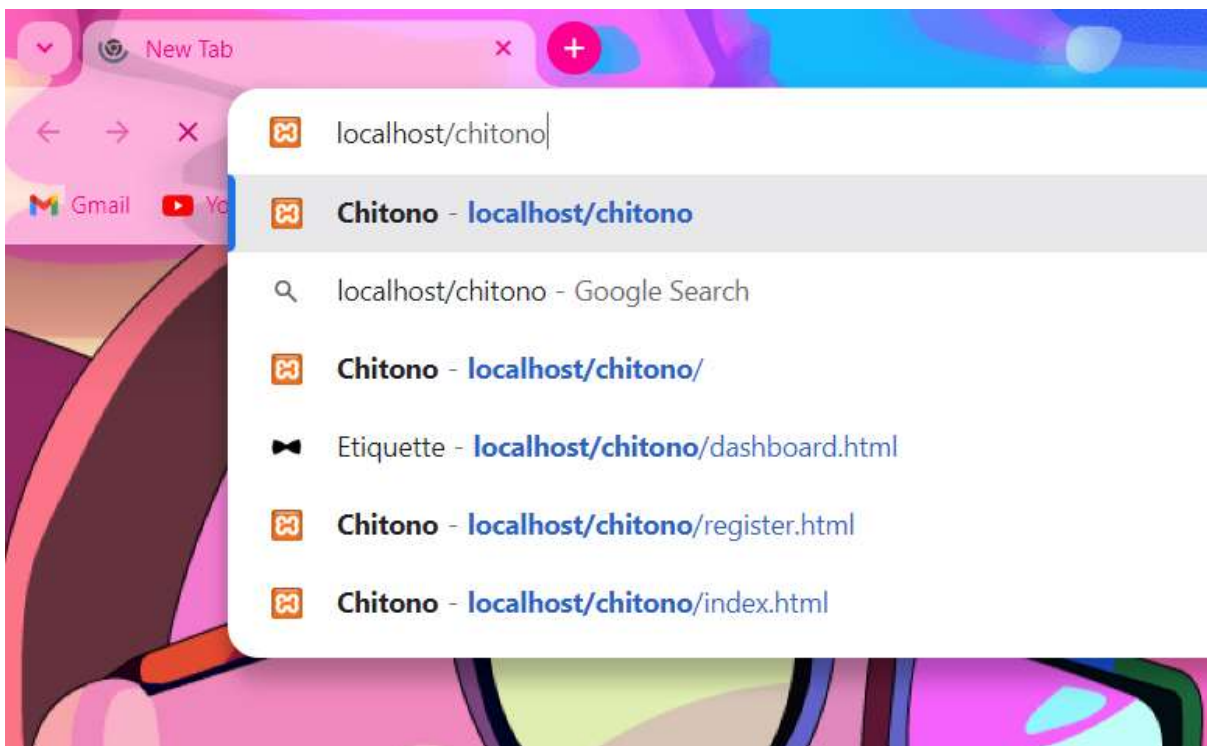


Figure 3: web access for the localhost

4. System Access

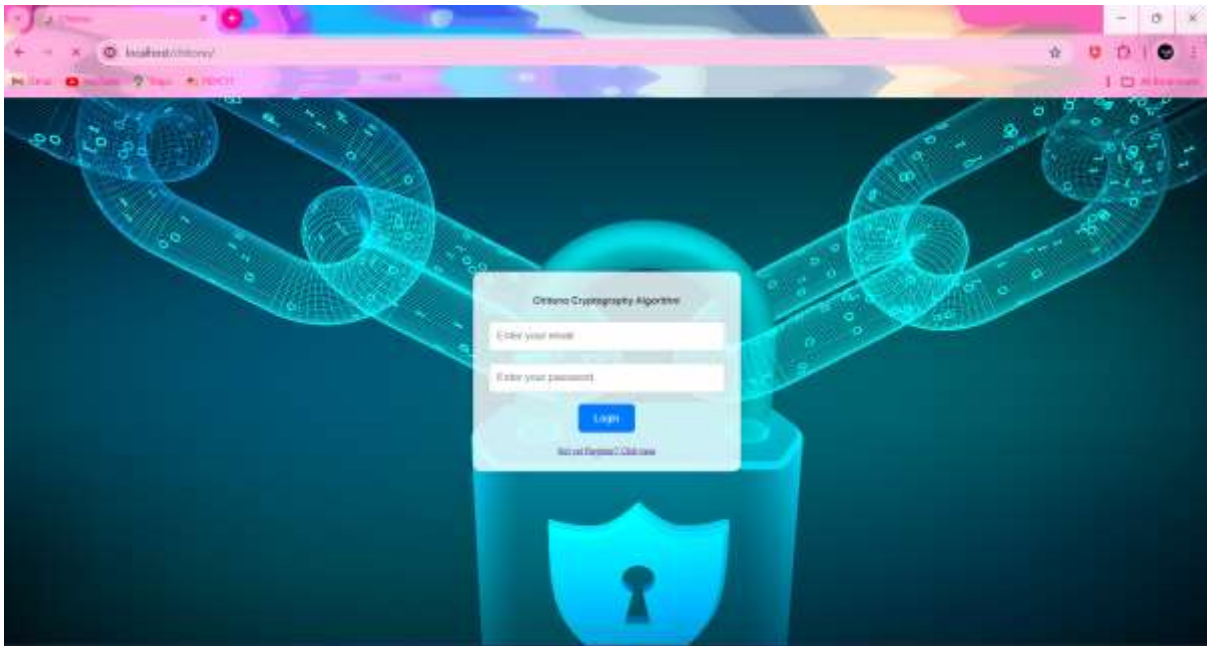


Figure 4: login page

The diagram above shows the page where a user can access the system through logging in there details or registering for a new account for entry into the ERP cryptography environment.

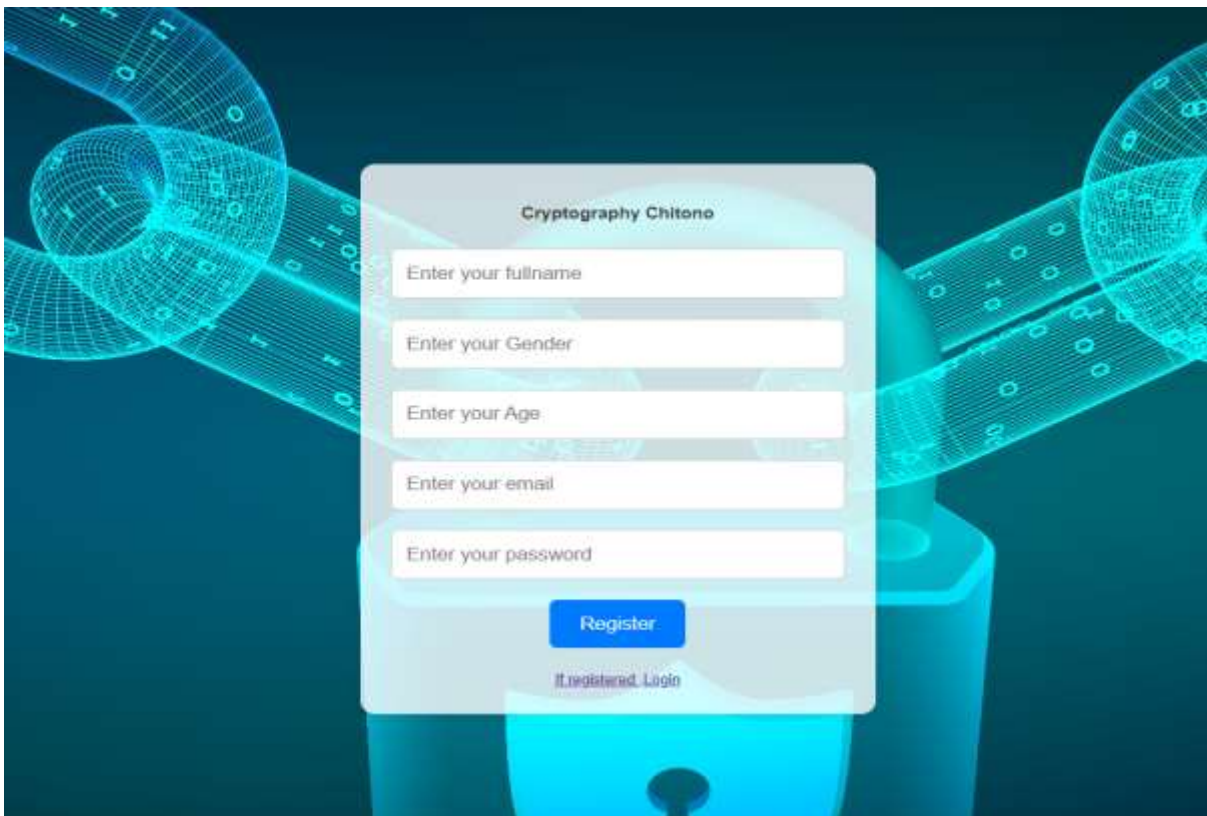


Figure 5: Registration page

The diagram shows the page where a new user can register to gain access to the system

Figure 6: The administration database

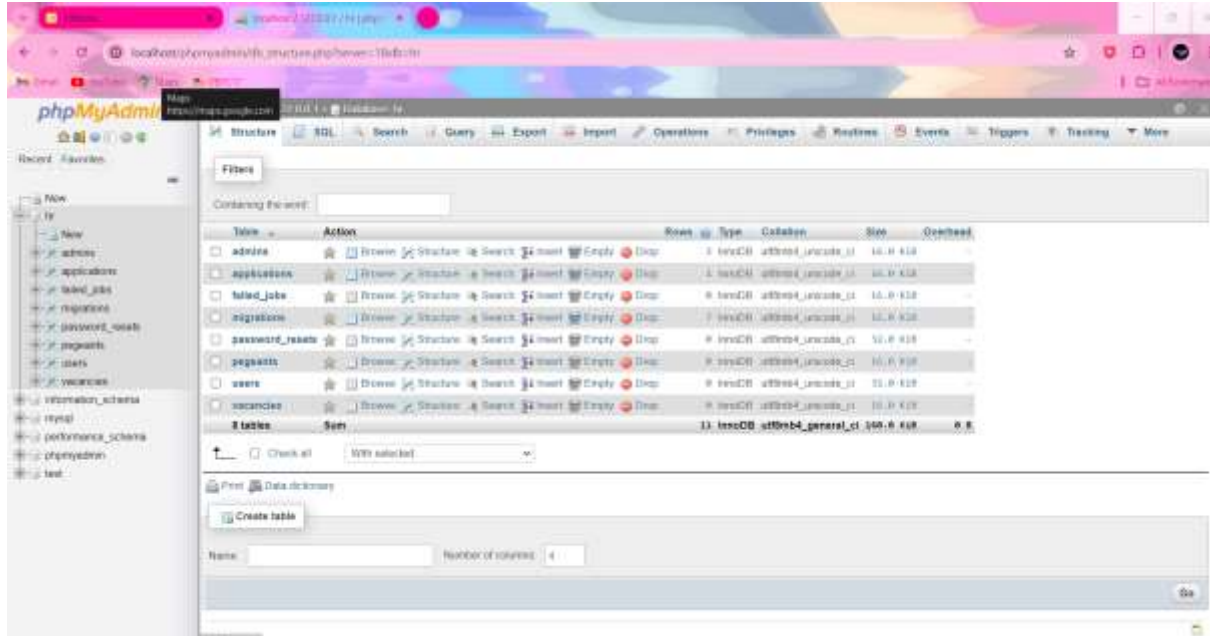
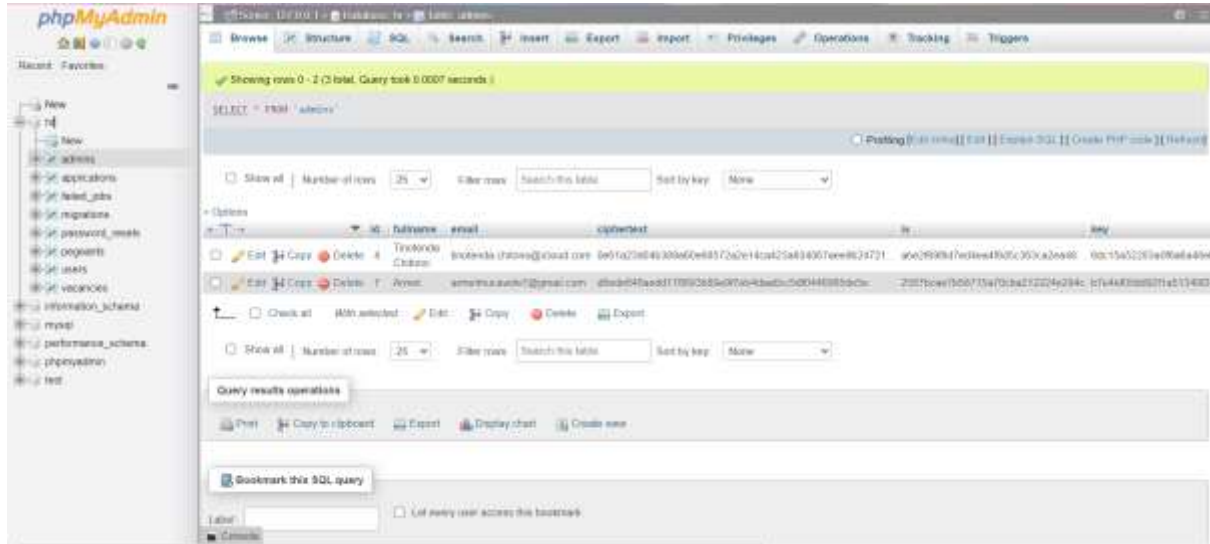


Figure 7: Cypher text page



This figure is the page where the cypher text In the admin database is inserted to access the system

Figure 8 : Admins in database



This is database where the ciphertext, iv, key passwords are kept

Figure 9: Cypher key

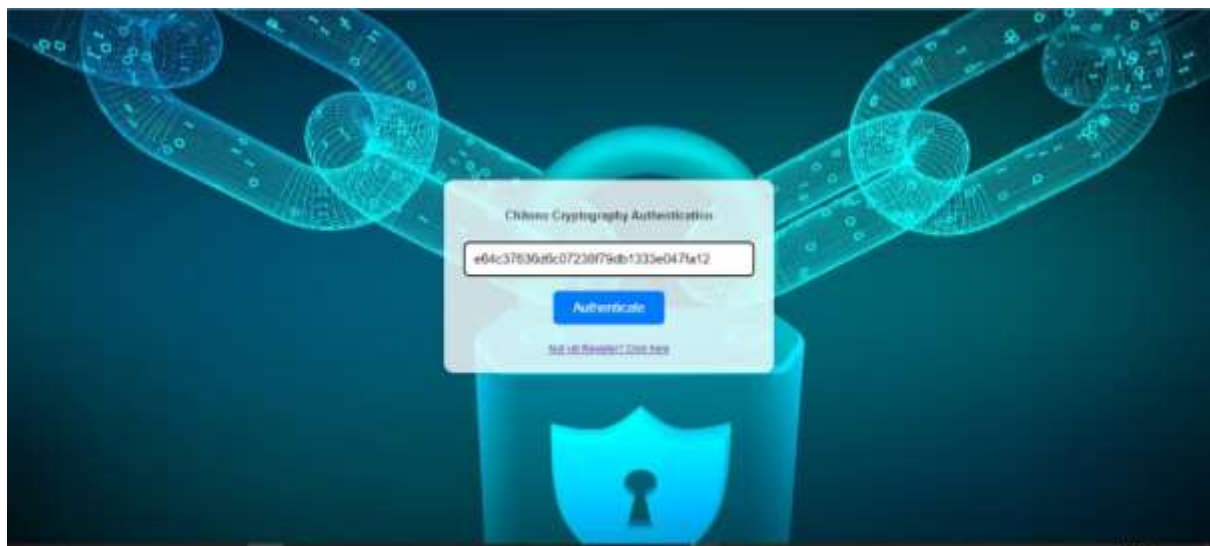


Figure 10: interface of the system

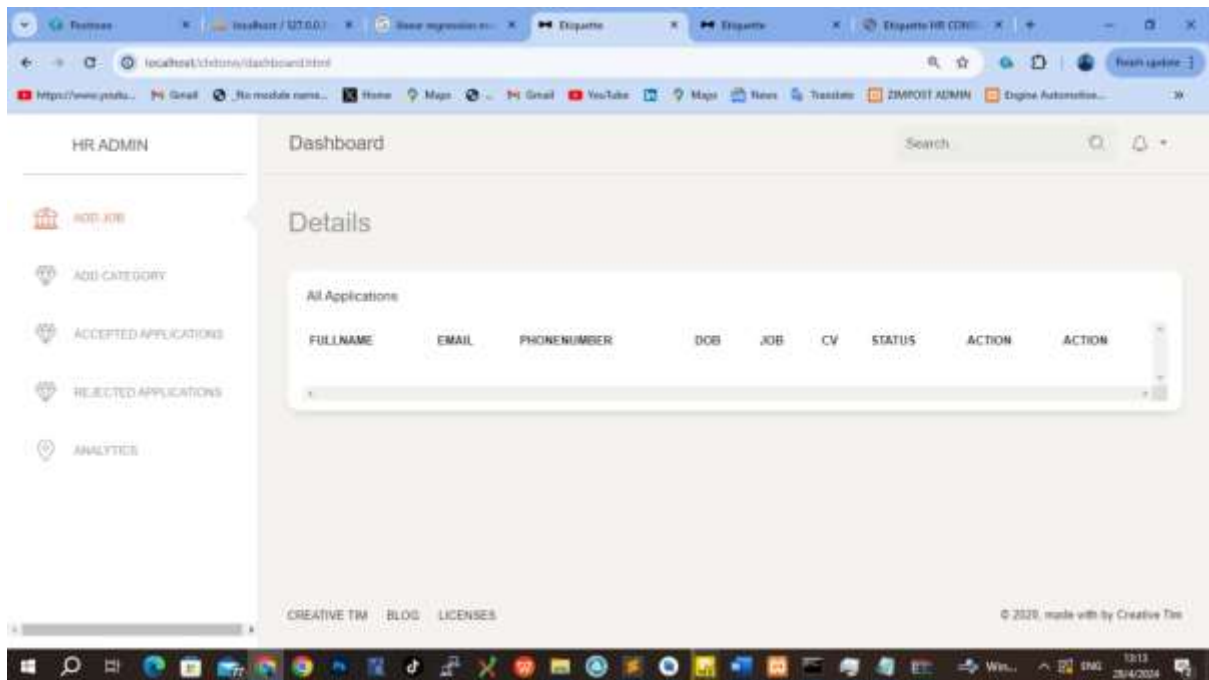
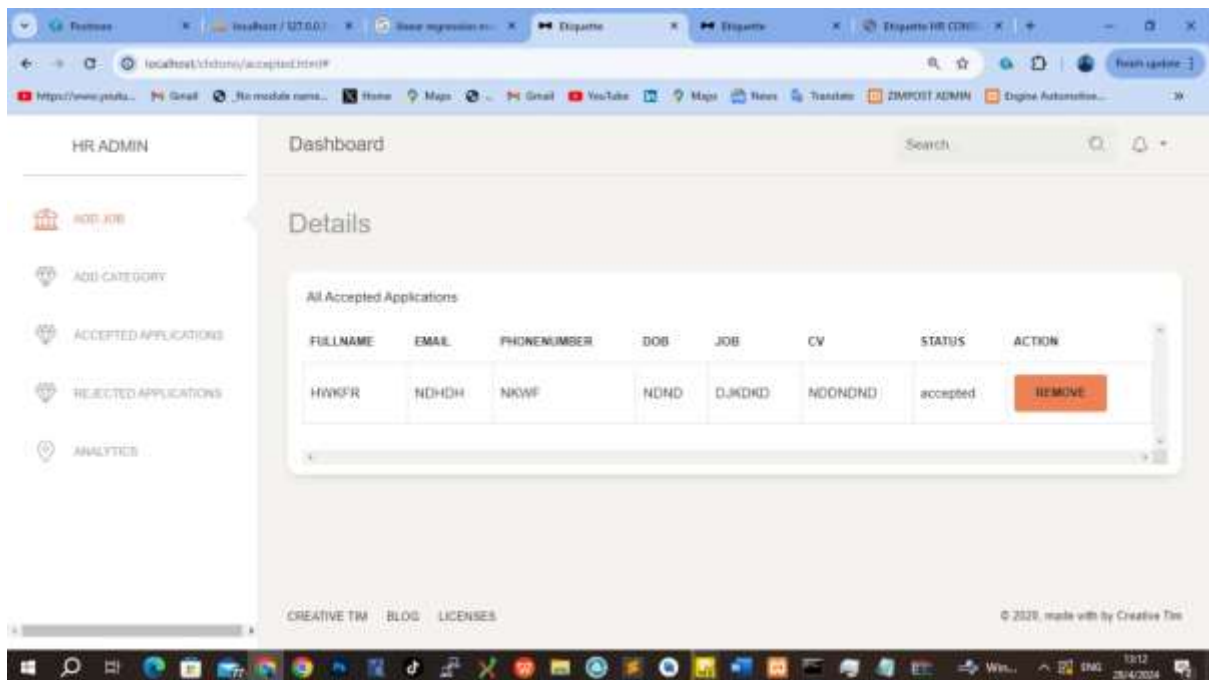


Figure 11: 7Dashboard



Chapter 5: CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

Chapter 5 aims to provide a comprehensive overview of the research outcomes, reflecting on the original aims and objectives, and presenting the key conclusions drawn from the study. Additionally, it offers actionable recommendations based on the findings and suggests potential areas for future research. This chapter serves as a bridge between the current study's findings and future explorations that could build upon this work to enhance the field further.

5.2 Aims and Objectives Realization

The primary aim of this research was to develop and evaluate a hybrid cryptography model for intelligent ERP authentication. The objectives included analyzing existing cryptographic methods, designing a hybrid model, implementing it in a controlled environment, and evaluating its effectiveness in terms of security and efficiency. Through extensive literature review, practical implementation, and rigorous testing, these objectives were systematically addressed. The hybrid cryptography model demonstrated improved security by combining the strengths of both symmetric and asymmetric encryption. The evaluation metrics indicated that the model not only enhanced data confidentiality and integrity but also maintained operational efficiency, thereby successfully realizing the aims and objectives set forth at the beginning of the study.

5.3 Conclusion

This research has established the viability and advantages of using a hybrid cryptography approach for ERP authentication. By leveraging symmetric encryption for its speed and asymmetric encryption for its security, the hybrid model provides a robust solution to the challenges faced in secure ERP systems. The findings suggest that hybrid cryptography can significantly improve the security posture of ERP systems without compromising performance. This study contributes to the field by providing a detailed implementation and evaluation framework that can be used as a reference for future developments in secure ERP systems.

5.4 Recommendations

Based on the research findings, several recommendations can be made to organizations looking to enhance the security of their ERP systems. Firstly, organizations should consider integrating

hybrid cryptographic models to leverage the combined benefits of symmetric and asymmetric encryption, thereby enhancing data security. Secondly, it is crucial to implement robust key management practices, including regular key rotation and secure key storage, to mitigate the risk of key compromise. Thirdly, establishing continuous monitoring mechanisms to detect and respond to security breaches promptly is essential. Additionally, conducting regular training sessions for users to ensure they understand the importance of security measures and follow best practices is recommended. Finally, encouraging collaboration between the IT security team and other departments can ensure comprehensive security measures are in place and properly followed.

5.5 Future Work

While this study has provided significant insights into the use of hybrid cryptography for ERP authentication, there are several areas where further research could be beneficial. Future studies should focus on testing the scalability of the hybrid cryptography model in larger, real-world ERP environments to ensure its efficacy across various scales. Investigating the use of more advanced cryptographic algorithms and techniques could further enhance the security and efficiency of the hybrid model. Exploring the integration of hybrid cryptography with other security measures such as multi-factor authentication and biometric verification can provide a more comprehensive security solution. Research into ways to optimize the performance of the hybrid cryptography model, particularly in resource-constrained environments, would be valuable. Lastly, assessing the impact of the hybrid cryptography model on user experience and identifying ways to minimize any potential negative effects while maintaining high-security standards is an important area for future exploration.

Appendices

Tinotenda Chitono Dissertation compiled.docx

ORIGINALITY REPORT

8%	6%	3%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	3%
2	liboasis.buse.ac.zw:8080 Internet Source	1%
3	Submitted to University of Maryland, Global Campus Student Paper	1%
4	ebookreading.net Internet Source	1%
5	1library.net Internet Source	<1%
6	Submitted to Wawasan Open University Student Paper	<1%
7	mymedr.afpm.org.my Internet Source	<1%
8	hdl.handle.net Internet Source	<1%
9	ir.unimas.my Internet Source	<1%

10	"Building Cybersecurity Applications with Blockchain and Smart Contracts", Springer Science and Business Media LLC, 2024 Publication	<1%
11	eprints.qut.edu.au Internet Source	<1%
12	"Fourth International Congress on Information and Communication Technology", Springer Science and Business Media LLC, 2020 Publication	<1%
13	Siva Raja Sindiramutty, Noor Zaman Jhanjhi, Chong Eng Tan, Navid Ali Khan, Bhavin Shah, Loveleen Gaur. "chapter 7 Securing the Digital Supply Chain Cyber Threats and Vulnerabilities", IGI Global, 2023 Publication	<1%

Exclude quotes On Exclude matches Off