ENHANCING DATA PROTECTION IN HEALTHCARE INFORMATION SYSTEMS USING CRYPTOGRAPHIC ALGORITHM WITH BASE64 512 BITS

Muthaura Agnes Kairuthi

Reg. No: J57/20620/2020

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT OF AWARD OF THE DEGREE OF MASTER IN SCIENCE COMPUTER SCIENCE IN SCHOOL OF PURE AND APPLIED SCIENCES OF KENYATTA UNIVERSITY

OCTOBER, 2024

DECLARATION

I Muthaura Agnes Kairuthi do hereby declare that this research dissertation is my original work except where references are made and this work has never been submitted to any other Institution for any award

Muthaura Agnes Kairuthi

J57/20620/2020

Signed..... Date.....

Supervisor's Declaration

This research dissertation report is submitted for examination with the approval of my supervisor.

Signed…….

Date.....

DR John Kandiri

Department of Computing and Information Science,

School of Pure and Applied Sciences,

Kenyatta University,

P.O. Box 43844-00100,

Nairobi, Kenya

DEDICATION

I dedicate this research work to my lovely husband Lazarus Ichaba who has been my source of strength and encouragement throughout this study. I also dedicate this work to my three little angels Isaac, Becky and Gian, thank you for your perseverance and endurance.

ACKNOWLEDGMENT

I would like to thank Almighty God for the serenity and peace to pursue this course to completion and for the grace to finish this dissertation report. I recognize the efforts of my supervisor, Dr. John Kandiri, for his support and guidance while writing this dissertation. More specially, I would like to appreciate the Dean, Faculty of Pure and Applied Sciences, Kenyatta University, for the great support made to see this work come through! May the almighty God and giver of all good things reward you abundantly and beyond. My dear husband Lazarus Ichaba and my adorable angels Isaac, Becky and Gian thank you very much for endurance and understanding. To my dear parents Mr. and Mrs. Muthaura, I sincerely appreciate your encouragements and prayers throughout my education life and your unwavering reassurance of my success. Gratitude to Peter Njuguna and Billy Kiseu who offered technical and moral support whenever there was need. May the Almighty God bless you all and May His face shine upon you all Amen!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

1. **MAC-** Mandatory Access Controls
2. **RBAC-** Role Based Access Controls
3. **DAC-** Discretionary Access Controls
4. **LBAC-** Label based Access Controls
5. **AES-** Advanced Encryption Standard
6. **EMR-** Electronic Medical Records
7. **BLP-** Bell La Padulla
8. **ICT-** Information Communication Technology
9. **OTP-** One Time Password
10. **MD5-** Message Digest Algorithm
11. **TDE-** Transparent Data Encryption

ABSTRACT

To avoid information leakage in healthcare information systems, patient data which is very confidential must be protected at the application level and at the data level as leakage of this information leads to serious medical legal issues. As the number of medical records stored electronically increase, enhancement of how this data is secured must be considered. Cryptographic algorithms are the most preferred data protection techniques for protection of sensitive and critical data such as health care data at the data level. Criminal assaults in social insurance have exponentially increased and are now the leading cause of medical data breaches. About all healthcare organizations have encountered no less than one data breach, costing million dollars on average per healthcare organization. In this study, design science research methodology was used to design and develop a cryptographic algorithm with Base64 512 bits to enhance health care data protection at the data level. The developed algorithm was tested and piloted in a healthcare facility through experiments and simulations by Senior Database Administrators, Senior Security Officers and System Administrators. The source of data for this study was obtained from secondary sources which involved collection of data from extensive literature review on the existing cryptographic algorithms. Analysis of the existing cryptographic algorithms were evaluated in depth and a criterion was obtained that determined how the most preferable cryptography algorithm would be improved to enhance data protection. The security parameters identified from the existing cryptographic algorithms were further classified and used as the inputs for the study. The outcomes of the developed cryptographic algorithm were interacted several times until the desired results were obtained. The performance of the developed cryptographic algorithm was evaluated for security measures such as brute force attack, known plain text vulnerability, database performance and use of private key. The results of the observations showed that the developed cryptographic algorithm with Base64, AES with fixed length of 512 bits achieved optimal performance on brute force attack, known plain text vulnerability and database performance. Thus, the addition layer of Advanced Encryption Standard with a fixed key length of 512 bits on the developed cryptographic algorithm enhanced on the data protection at the data level. In conclusion, to ensure improved data protection in healthcare information systems cryptographic algorithms at the data level should ensure proper encryption and decryption of data and appropriate access control. The cryptographic algorithms must meet the mandatory security features such as low Known plain text vulnerability, use of private key, strength on brute force attack and ease of decryption and encryption.

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE STUDY

1.0 Introduction

Healthcare Information System is a system that is used in a healthcare facility to capture and store patient's data (Medical, 2023). In most cases these systems are classified as distributed systems because they are connected to several other systems and networks for proper management of patient data (Boulahia-Cuppens et al., n.d.). To avoid information leakage, patient data which is very confidential must be protected at the application level and at the data level as leakage of this information leads to serious medical legal issues. As the number of medical records stored electronically increase, enhancement of how this data is secured must be considered. (Ge et al., n.d.). Delay in the retrieval of patient records at the right time can cause death and also lower the level of health care services offered by the healthcare facility (Babatunde A). Criminal assaults in social insurance have exponentially increased since 2010 and are now the leading cause of medical data breaches (Babatunde et al., n.d.). About all healthcare organizations have encountered no less than one data breach, costing million dollars on average per organization (Ed Oswald, 2022).

The level of security and data protection in Healthcare Information Systems varies from one healthcare facility to the other(Ahmed et al., 2018). Healthcare Information Systems are generally integrated with Electronic Medical Records. The health information system stores bio data of the patient which include name, sex, gender, religion, marital status, date of birth and many more and Electronic Medical Record system stores the clinical data for the patient such as vital signs, allergies, diagnosis,

investigations, medications, assessment, recommendations and patient medical history (Lucca et al., 2020).

The patient data stored as clinical data is the most sensitive data that must be encrypted using an enhanced cryptographic algorithm and secured with a private key (Rajab et al., 2021)The existing data protection models and database security methods and techniques focus more on protection of data on subjects (users) access to the system and less focus on objects(data) protection at data level (Soe & Phyu, n.d.)The implementation of data protection at the database level is generally configured as a default setting such as Mandatory Access Controls (Bell La Padulla models, Biba Models, Clark & Wilson models) (Lee et al., 2020) Electronic Medical Records in Healthcare Information Systems must be protected using enhanced cryptographic algorithm at the data level.

1.1 Background of the study

Data protection in Healthcare Information Systems at the data level is very critical and sensitive and it offers privacy and confidentiality of patient data and information. Patients' data must be protected from access control level, the front end and at the database level, the backend(Paragas, 2020). There has been an increase on the use of technology in healthcare sector and thus increased use of Healthcare Information Systems. This has also led to an increase in cybercrimes in Healthcare Information Systems (Lee et al., 2020) and this calls for improved data protection algorithms in healthcare data using enhanced Cryptographic Algorithms.(Diamantopoulou et al., 2017) Data protection in Healthcare Information Systems focus more on the access control level (application level) and less focus at the data level (Database level) thus allowing a very huge risk of data exposure for patient data at the database level or the

backend. An attacker can easily hack the log in details and access the system through frontend by simply decrypting the passwords and if the patient data is not encrypted at the backend using enhanced cryptographic algorithms the information will be accessible by an unauthorized user(George & Bhila, 2019a). There is existence of cryptographic algorithms used in Healthcare Information Systems at the access level and database level but there is need for enhancement using enhanced cryptographic algorithm proposed in this research. It is estimated that thousands and millions of personal data and information of patients is leaked especially on their credit cards and bank details. ((Paragus, 2020). Healthcare facilities and public health sector invests quality time in the data lifecycle (Paragus, 2020)

The General Data Protection Regulation goal is protection of sensitive or confidential data and unforeseen risk of data loss or theft (2019_kenya, 2019), encryption makes sure that all confidential or sensitive information is protected by an agreeable security level at the destination and at the source. (Lucca et al., 2020). Therefore, the motivation of this study was to design and develop a cryptographic algorithm that would ensure data protection in health care information systems is securely stored and retrieved(Sanas et al., 2020. The developed cryptographic algorithm would have advanced cryptographic features that would enhance data level protection in health care systems(George & Bhila, 2019b). These features would ensure a low risk on known plain text vulnerability, increased strength on brutal force attack, use of private key and improved database performance.(Sanas et al., 2020) The implementation of the developed advanced cryptographic algorithm will significantly reduce the current problem on data level leakages in healthcare systems. (Babatunde et al., n.d.)

1.2 Problem Statement

Despite innovations and advancement in cybersecurity in Healthcare Information Systems, data level protection for patient sensitive data still remains vulnerable to cyberattacks and data breaches. Currently there lacks a holistic cryptographic algorithm that can protect all patient data at the data level. Existing data-level protection techniques that are developed to ensure data-level protection in Healthcare Information Systems lack integration of key security models such as Mandatory Access Controls, Role Based Access Controls and database security approaches such as Authentication based security, Trust based security and preferred major parameters and characteristics for cryptographic algorithms in the design and development of cryptographic algorithms. Patient data is in the category of the most sensitive data and can cause enormous issues including patient's death and life imprisonment for healthcare personnel. The world of technology is growing very fast in every sector and more aggressively in healthcare sector due to the high uptake of medical health insurances and life insurances by individuals and corporates. The insurance data and the patient data are generally integrated for proof of patient identification to enable the patient access to medical care. On the other hand, the cybercriminals are also growing at the same rate as the technology and therefore institutions that store sensitive data especially health facilities, insurances, military and some government institutions must explore techniques and tools that will minimize the rate of data level exposure to cybercriminals. Cryptographic algorithms mainly ensure encryption and decryption of data for storage and retrieval in the database. The process of data encryption in a healthcare information system should be fast to promote improved patientcare and the decryption process must also be very fast to ensure that the data is retrieved at the most

optimal time. In most healthcare information systems, the process of data decryption slows down database performance due to lack of automation of database re-indexing of tables, columns, rows and views for optimal database performance. A delay in patient data retrieval or data capture can lead to death of a patient and this leads to a rise in medical legal cases. A preferred healthcare information system database must be optimized to perform at an optimal speed whereas this action is mainly ignored or left out during the system design phase and development of cryptographic algorithms. Healthcare information system should have a clear well-defined role matrix to ensure that specific users and applications can only access what is relevant to their roles, thus role-based access controls and mandatory access controls must be incorporated in the design and development of a cryptographic algorithm. This improves on user management in the mapping of roles and permissions for access to the database as well as database monitoring and auditing. This strengthens brute force attack and lowers the risk of known plain text vulnerability in healthcare information systems. Brute force attack and known plain text vulnerability are currently ranked the top cybercrime attacks in healthcare information system. These attacks are mainly in form of ransomware whereby the cybercriminals gain access to the database and hold the database hostage or expose the sensitive data to the internet also known as dark web. This leads to financial and reputational loss for a healthcare facility. The existing algorithms are inadequate in data protection at the data level as the algorithms only checks security at the data entry level. Therefore, there is a strong need to design and develop an algorithm that checks data security at the data level. This study endeavored to design and implement a cryptographic algorithm with Base64 512 bits. This is envisaged to enhance data level protection in healthcare information systems. Further,

the study endeavored that the additional encryption layer with Base64 algorithm and Advanced Encryption Standard with a fixed key length of 512 bits would strengthen brute force attack and lower the risk of known plain text vulnerability. Further, it is believed that automation of database optimization for healthcare information systems in the configuration of cryptographic algorithm with Base64 512 bits would improve on database performance and patient care.

1.3 Justification

In this research, the design, development and implementation of the enhanced cryptographic algorithm will improve patient data protection (confidentiality and integrity) at the data level in Healthcare Information Systems. A mandatory requirement for Healthcare Information Systems as stated in ISO2799 in Health Informatics The recent frequent data breaches in health care systems will be reduced significantly when the implementation of the study is adopted by health care facilities. The research will facilitate the Government of Kenya in implementation of Data Protection Act 2019. The positive results of the research will be advocated for use in healthcare facilities to improve on the existing cryptographic algorithms at the data level. The research will benefit medical researchers in their studies during data collection phase as the data access levels will be controlled.

1.4 Objectives

1.4.1 General Objective

The purpose of this study was to design and implement cryptographic algorithm with base64 512 bits to enhance data protection in Healthcare Information Systems.

1.4.2 Specific Objectives

1. To investigate the existing data encryption algorithms in Healthcare Information Systems and their security characteristics for data protection at the data level
2. To evaluate data protection techniques in Healthcare Information Systems at the data level for integration in the design of the cryptographic algorithm with Base64 512 bits
3. To design an enhanced cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems
4. To evaluate the performance of the cryptographic algorithm with Base64 512 bits in protecting data in healthcare systems

1.5 Research Questions

1. What is the main existing data level cryptographic algorithms in Healthcare Information Systems
2. What are the major data protection techniques in Healthcare Information Systems at the database level
3. How is the performance of the developed cryptographic algorithm with Base64 512 bits for data protection in healthcare information systems.
4. How does encryption and decryption of data at the data level affect the performance of the database and how can this be optimized

1.6 Significance of the study

From the findings of this research, patients will be the first beneficiaries since their most confidential and sensitive data will be safe and secure from any unauthorized access. Medical Practioners will benefit from the drastic reduction of medical legal cases and thus improvement in the Patient-Doctor relationship. The Medical

researchers will benefit from this research as they will have access to the relevant data for their studies and in the most secure way. Most medical research projects take a long time to be completed because acquisition of data for research on healthcare information systems is most difficult to access due to patient data confidentiality. The Healthcare sector will invest more on Electronic Medical Records in Healthcare Information Systems and thus improved Healthcare services to the patients and this will boost revenue generation in Healthcare centers. This study examined that enhancing cryptographic algorithms at the database level improves on the data privacy in healthcare information systems. The proposition of implementing this project study will be a great achievement in providing a solution to data protection and privacy of sensitive data at the database level in healthcare information systems.

1.7 Scope and Limitation

Although protection of data in Healthcare Information Systems involves protection of data on transit (security over the network), the data at rest (database security), backup data (data for recovery and restoration). This research focused on data at rest (data stored in the database). Research tended to classify the features and characteristics of data that need to be more secure in a Healthcare Information System. This research did not involve network security and disaster recovery techniques and backup security. This research was based on literature review and therefore the data for analysis was from secondary sources.

1.8 Assumptions

- Cryptographic algorithms are too expensive and difficult to implement at the data level

- Cryptographic algorithms affect the performance of a system if all the data in the database is encrypted when the decryption of data is necessary.
- The mathematical and computational techniques used to design and develop cryptographic algorithms can be manipulated to enhance data protection and confidentiality at the data level.

1.9 Theoretical framework

Studies have grouped access control into three categories: The first category is the access controls that control subjects (users) only such as Role Based Access Control. The second category is the techniques that aim at strengthening or enhancing the security of the objects (data). These techniques are masking, Digital water marking, image fusion and encryption. The third category of access control considers both objects and subjects such as Mandatory Access Control models (Lee et al., 2020). These categories of access control do not really provide sufficient data protection for the objects which is primarily their main goal and objective. Instead they focus either on integrity (Biba Models) or confidentiality (Bell La Padulla models). In addition, the MAC models which include Biba Models, Bell La Padulla models and Lattice Based Access Control models do not describe any cryptographic algorithm for enhanced data protection. Although LBAC was emphasized to be able to solve this problem mathematically by use of information flow when used in combination with Biba models and BLP models the encryption of (data) objects is not considered. (Lee et al., 2020).

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter contains detailed literature review of the existing cryptographic algorithms on the theoretical and empirical frameworks, database approaches and securities, healthcare information system vulnerabilities and the various security models. Cryptography is the study of mathematical calculations and techniques, cryptography function transfers plain text into cipher text (encryption) and transfers cipher text into plain text(decryption) Some refer Cryptography to “secret writing” (Rajab et al., 2021)

The plain text is encrypted to cipher text and decrypted into plain text using a security key or security keys, enhancing data protection in Healthcare Information systems is a mandatory requirement and a sensitive activity that requires protection of both subject (users) and objects (data) (Paragas, 2020). The patient data and information must be secured from application access control level to database access control level. This guarantees security of sensitive data and information from end to end and improves on patients care and user experience. The following modern and existing cryptographic algorithms were reviewed and evaluated in this study.

2.1 Hill Ciphers

This is one of the oldest cryptographic algorithms that was developed by Leiser Hill in 1929 and uses mathematical manipulations such as linear Algebra.(Vijayaraghavan#1 et al., 2018) To enhance the algorithm, matrix manipulation is used and uses Mod26. This means the alphabets A to Z are substituted with numbers or integers 1 to 26 to encrypt and decrypt data. Unfortunately, this algorithm has high known plain text

vulnerability.(Paragas et al., 2019) Studies show that Hill cipher has been modified using mathematical manipulations to strengthen the algorithm from known plain text vulnerability attack and brutal force attack(Vijayaraghavan#1 et al., 2018). From this study the author identified the Modified Hill cipher to have a higher avalanche effect as compared to the original hill cipher. Avalanche effect was the results of the experiment to test the effect of change on the cipher text. This experiment showed that 54 percent of change was affected on the cipher text as compared to the original hill cipher whose effect on change was 100 percentage(Paragas et al., 2019). This meant that by mathematical manipulation on the original hill cipher made it more difficult to make changes on the cipher text and thus Modified hill cipher was considered for enhanced data protection. Despite this modification the algorithm is vulnerable to known plain text, uses a private key and its performance is slow on decryption of the encrypted data

2.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard 256-bit encryption is the most secure encryption standard available. It uses a 256-bit key length and is widely used in symmetric encryption as a highly secure and robust option for data protection(Ed Oswald, 2022). In cryptography the longer the bit key length the stronger and secure the algorithm. Mostly referred to as the gold standard for data encryption, AES is used by many government bodies worldwide, including in the U.S.AES block cipher encrypts 128-bit data blocks at a time. (Application Research of Data Encryption Technology in Computer Network Information Security," 2023)AES has a limitation that relates to the decryption process implemented in different settings. AES encryption uses a "symmetric block cipher" or encryption algorithm developed by the National Institute

of Standards and Technology (NIST) in 1997 to make government data less susceptible to brute force attacks. It splits the message into smaller blocks instead of single encryption round, including substitution, transposition, and mixing(George & Bhila, 2019a). A 128-bit key undergoes 10 rounds of encryption, while a 192-bit key uses 12, and a 256-bit key uses 14 rounds. The result is effectively impossible to crack using a brute-force attack with today's computers. When implementing software, the inverse operation requires different codes and tables thus slowing the process of decryption. Limitations to AES algorithm are related Key attack which occurs when a hacker studies how an AES cipher operates with different keys and tries to crack it that way. Researchers say that properly configured AES systems are not vulnerable to related-key attacks.(Ed Oswald, 2022) Side-Channel Attack which occurs when the attacker collects data on what a computing device does while performing cryptographic functions. This information is then used to reverse engineer the cryptography system. Known-Key Attack which happens when the attacker knows the keys used in the cipher.

2.3 Triple Data Encryption Standard (3DES)

This is a symmetric encryption algorithm that uses 54 -bit key to encrypt data blocks. This is more secure version of Data Encryption Standard algorithm and applies DES to each block of data three times. (Raza, 2023)This algorithm has a short bit key length thus increased known plain text vulnerability. Triple Data Encryption Standard (3DES) was made from DES calculation, developed in the mid-1970s utilizing 56-bit key.(Babatunde et al., n.d.) The powerful security 3DES gives just 112 bits because of meet-in-the-centre assaults. Triple DES runs three times slower than DES, however is significantly more secure if utilized appropriately. The methodology for unscrambling something is the same as the technique for encryption, aside from it is executed

backward. Triple DES calculation utilizes three emphases of normal DES figure. It gets a mystery 168-piece key, which is partitioned into three 56-bit keys. The buildup of 3DES compasses of Encryption utilizing the primary mystery key, Decryption utilizing the second mystery key, Encryption utilizing the third mystery key.

2.4 Two fish

Two fish is a symmetric-key block cipher with a block size of 128 bits and variable-length key of size 128, 192 or 256 bits. It is optimized for 32-bit central processing units and is ideal for both hardware and software environments and similar to an earlier block cipher, Blowfish. (Rahul Awati, 2021)It also includes advanced functionalities to replace the Data Encryption Standard (DES) algorithm. Published in 1998, Twofish was among the finalists in a competition to determine the best block cipher algorithm to replace DES. The competition was organized by the National Institute of Standards and Technology. However, Twofish lost out to the Rijndael algorithm as the best possible alternative to DES, mainly because, although Twofish is secure, it is slower than Rijndael. (Rahul Awati, 2021)Twofish, being a symmetric encryption algorithm, uses a single key to both encrypt and decrypt data and information. It accepts the key along with the plaintext information. This key then turns the information into ciphertext, which cannot be understood without decoding. The encrypted data is sent to the recipient along with the encryption key, either after the ciphertext or with it. The user can use this key to decrypt the encrypted information. With a 128-bit block size and variable-length encryption key, Twofish is one of the most secure encryption protocols. In theory, its high block size means that Twofish is safe from brute-force attacks, since such an attack would require a tremendous amount of processing power to decrypt a 128-bit encrypted message.

It is argued that the precomputed, key-dependent S-boxes used in Twofish are vulnerable to attacks. (Rahul Awati, 2021)However, it is possible to minimize the risk of a side-channel attack by making these tables key-dependent. Despite a few attacks on Twofish, its creator, Bruce Schneier, believes that they were not practical breaks, which again reiterates that Twofish is an exceptionally secure encryption algorithm. The complexity and intensive resource utilization for this algorithm has limitations on its implementations.(Rahul Awati, 2021)

2.4 Security Models

There exist several security models that enhance data protection at the application access level such as OTP (One Time Password) and database access control level such as Mandatory Access Control models. These are the access control methods for Database security that focus only on confidentiality and integrity (Paragas, 2020). The other models that enhance data security include Bell La Padulla Models and Biba Models. Traditional data protection techniques such as masking, Image fusion, digital water marking and encryption are an expansion of Discretionary Access Control. DAS restricts access to objects(data) based on the identity of the subject(user).(Ferraris et al., 2023) Role Based Access Control, aims at strengthening the security of data but only from the subject (user) access control level. RBAC restricts network access based on the roles of individual users within an enterprise. (Vijayaraghavan#1 et al., 2018)Thus, the traditional data protection models and access controls lack enhanced cryptographic algorithms to protect sensitive data in healthcare information systems at the object (data) level and that are very complex without compromise especially in this era of high increase in cybercrimes.(Lucca et al., 2020) Data protection in healthcare information system can be enhanced by use of enhanced cryptographic algorithm that validates the

subject (user) on access at the application level to the (Object) database level by encryption and decryption of the patient data.

2.5 Database Security in Healthcare Information Systems

There exist access control methods for database security such as Mandatory Access Control (MAC) model in which the security level is set to both the subject and the object to enhance the security control. The legacy MAC models have focused only on one thing, either confidentiality or integrity. (Lee et al., 2020a)Database security is incorporated in every database and has several layers and with the security types such as access control, auditing, authenticating and encryption.(Mohamed et al., 2022) Database security approaches in Healthcare information systems classified as authentication-based security, trust-based security approaches, access control (DAC, MAC and RBAC Models) based approaches and Cryptographic based approaches (a technique for securing database) (Rjaibi & Bird, 2004) lacks an enhanced data level protection algorithm to guard the data against the emerging advanced cyber-attacks techniques**.** This study examined that enhancing cryptographic algorithms at the database level improves on the data privacy in healthcare information systems. The proposition of implementing this project study will be a great achievement in providing a solution to data protection and privacy of sensitive data at the database level in healthcare information systems.

This study examined that enhancing cryptographic algorithms at the database level improves on the data privacy in healthcare information systems. The proposition of implementing this project study will be a great achievement in providing a solution to data protection and privacy of sensitive data at the database level in healthcare information systems.

2.6 Evaluation Criteria of Acceptable Cryptographic Algorithm

From the extensive literature review, an evaluation criterion was set up for an acceptable cryptographic algorithm. For a cryptographic algorithm to be considered for further progress in the study the following security features and characteristics were evaluated, strength on brute force attack, known plain text vulnerability, user of private Key, use of RBAC and ease of encryption and decryption. The strongest cryptographic algorithm on data protection was considered further for evaluation with the developed cryptographic algorithm with Base64 512 bits. An adequate cryptographic algorithm should have the following features and characteristics according to the authors and researchers as indicated in table 2.4. Table 2.4 summarizes the major security features and charateristics according to different authors point of view. From the literature review findings, five different authors and five cryptographic algorithms were selected for phase one evaluation of the study from a list of 100 authors and 20 cryptographic algorithms identified. Original Hill Cipher, Modified Hill Cipher, Advanced Encryption Standard algorithm,3DES, Two Fish encryption algorithm, and MAC and Enhanced Tiny Encryption cryptographic algorithms were evaluated. As Table 2.4 shows, Advanced Encryption Standard was identified as the strongest existing cryptographic algorithm. This informed further on details of enhancement of the AES cryptographic algorithm to improve data level protection in healthcare information systems.

Table 2.4 Evaluation Criteria Algorithm

Author/Year	Name of the Algorithm	Utilization of RBAC	Strength on brutal force attack	Known Plain text Vulnerability	Use of Private Key	Ease of data decryption and Performance
A Study on the Analysis of Hill's Cipher in Cryptography N. Vijayaraghavan1, Narasimhan, Baskar Mathematics Division, Department of Science and Humanities, KCG college of Technology, Chennai, India-600097- February 2018	Original Hill Cipher Algorithm	No	No	Yes	Yes	Yes
Paragas J, Sison A, Medina R 2019 IEEE 11th International Conference on Communication Software and Networks, ICCSN...	Modified Hill Cipher Algorithm	No	Yes	Yes	No	No
Onboardbase website by Basile https://onboardbase.com/blog/aes-encryption-decryption/#:~:text=AES%20is%20a%20symmetric%2Dkey,a%20secret%20key%20for%20decryption.	Advanced Encryption Standard Algorithm (Rijndael)	No	Yes	Yes	Yes	No
Soe A, Phyu S	Mandatory Access Control Algorithms (Biba,La padula,Clark Wilson)	Yes	No	No	No	No
Ahmed A, Abdulsalam Y, Olanivi OInternational Journal of Information Privacy, Security and Integrity (2018) 3(3) 230	Enhanced Tiny Encryption Algorithm	No	Yes	No	Yes	No

Adequate data level encryption algorithm must have at least the following features which include, utilization of RBAC, strength on brute force, known plain text vulnerability, use of private key and ease of data decryption and database performance. An evaluation criterion was used to test the adequacy of each security feature for each specified cryptographic algorithm at the data level. This determined how the enhanced cryptographic algorithm Base64 512 bits was designed and developed for adequate data level protection. The following step by step evaluation criteria was used to identify an adequate cryptographic algorithm as indicated on Table 2.5. The selected algorithms were tested for each security parameter as identified from the intensive literature review. A comparison study was conducted to choose the strongest algorithm.

2.4.1 Utilization of Role Based Access Control

This criterion evaluated whether the algorithm utilized RBAC. A good cryptographic algorithm should define users, roles, permissions and the level of database access. This feature ensured that only authorized users had access to the database and could perform specified roles and actions depending on the permissions mapped to their roles. When tested the algorithm should allow specific users to access specific levels of database according to their roles. These roles were created and mapped to respective permissions and then assigned to users. The users in this case were Systems Security Officers, Database Administrators, Network and Systems Administrators, ICT Officers, Nurses, Doctors, Health Information Officers, Radiologists, Pharmacists and Laboratory Technologists. The algorithm passed this criterion if it met all the parameters and scenarios subjected to the algorithm as per RBAC guidelines. These results were recorded for comparison with cryptographic algorithm Base64 512 bits.

2.4.2 Strength On Brute Force Attack

In this criterion the algorithm was evaluated to test its strength on brute force attack at the data level. The algorithm was tested to ensure that no penetration or data breach would occur. All generated passwords were to meet the set threshold to ensure that no guess password would penetrate the data level however several times an attacker could force. The algorithm was expected to perform encryption of the passwords and user names before they are saved in the database for enhanced data level protection. The algorithm that met this criterion was used for comparison with cryptographic algorithm Base64 512 bits.

2.4.3 Known Plain Text Vulnerability

An adequate cryptographic algorithm must ensure that the plain text that is encrypted to cipher text cannot easily be known. In this criterion each identified cryptographic algorithm was subjected to known plain text vulnerability test to find out its Avalanche effect. The vulnerability was tested and scored either as high risk, medium risk or low risk. The algorithm with low risk for known plain text vulnerability was considered for further experiments and comparison with cryptographic algorithm Base64 512 bits.

2.4.4 Ease of Data Decryption and Database Performance

A good cryptographic algorithm should be fast to encrypt and decrypt data at the data level thus ensuring high database performance. In this criterion the cryptographic algorithm was tested for database performance during data retrieval and how fast the data could be encrypted and decrypted. The results were recorded whether slow or fast database performance and the algorithm with fast database performance was listed for further analysis and comparison with enhanced cryptographic algorithm Base64 512 bits.

2.4.5 Use of Private Key

For enhanced data level security, a good cryptographic algorithm is necessary with a private key that ensures that the private key is utilized by authorized users. Each algorithm was tested for key length. The higher the number of bits of the key length the secure the key. This was to be achieved at the authentication of users by barring unauthorized users and applications to the database. For a cryptographic algorithm to be selected from this criterion it was to have a private key with a specified key length of 512 bits and above. The algorithm that met this criterion was selected for further analysis and comparison with the cryptographic algorithm Base64 512 bits.

Table 2.5 Comparison of Security features and characteristics of the existing cryptographic algorithms

Algorithm	**Strength on brute force attack**	**Key Length**	**Block Size**	**Rounds for Encryption**	**Level of Vulnerability**
Twofish	Strong	128,192, 256	128	16	Low
AES	Strong	128,192, 256	128	14	Medium
TDES	Weak	64	128	12	High
DES	Very Weak	56	64	10	Very High

As illustrated on Table 2.5, the strength on brute force attack, key length, block size, rounds for encryption and the level of vulnerability for each algorithm identified for study from literature review. As Table 2.4 illustrates, AES emerged the strongest existing cryptographic algorithm for further evaluation. The developed enhanced cryptographic algorithm with base 64 512 bits was designed, developed and compared with AES for data protection at the data level.

Figure 2.4 illustrates cryptographic algorithm evaluation model that was used to identify the best fit cryptographic algorithm. The figure shows a step by process of identification of the preferred cryptographic algorithm for further study. At the start is where the process begins for subjecting each individual algorithm to all the set criteria for security features and characteristics as indicated on Table 2.5. The other stages on figure 2.4 involve specific security parameter such as RBAC, brute force attack, known plain text vulnerability, use of private key and database performance. The result stage indicates the outcome of each algorithm and ends the process.

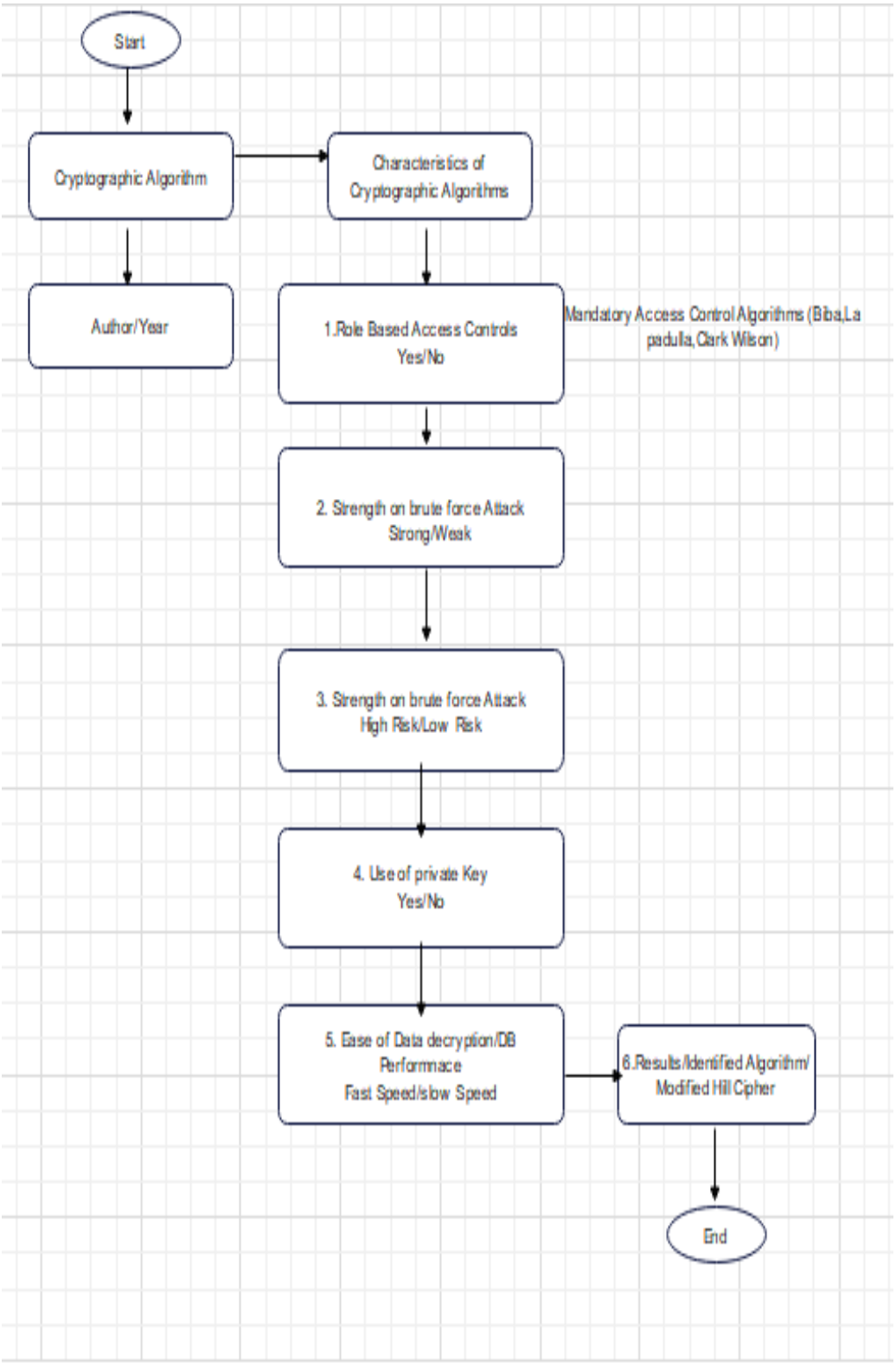


Figure 2.4 Evaluation Criteria Model

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter describes detailed research design methods and methodology in a systematic way on how cryptographic algorithm Base64 512 bits was designed, developed, tested and deployed for data protection in healthcare information systems. The methodology that was used to develop the cryptographic algorithm Base64 512 bits was the design science research methodology. This research methodology was best suited for this research because it combined both mathematical and computational methods that assisted in developing the algorithm. This contributed to measuring the quality of developing the artifact. It is based on guidelines that are branched from several science disciplines and this made the integration of security models and database security approaches simple during the implementation phase. It adopts proof methods of verification as opposed to existing empirical methods and this enabled extensive testing of the artifact and thus accurate results.

3.1 The Design Science Approach in Research Methodology

This research work adopted the design science approach as the research methodology because primarily it involved studying of existing security frameworks such as MAC Models (Biba, Bell La Padulla, Clark Wilson) (Lee et al., 2020a)and the existing database security methods such as various cryptographic algorithms (Symmetric and asymmetric) and access controls such as RBAC and DAC. The research studied how security algorithms have been implemented in healthcare facilities and in theories on literature review. The study analyzed the existing security algorithms, their features and characteristics in data protection for enhanced security at the data level. The results of the analysis of the existing

security algorithms determined how the artifact was developed. The developed model was evaluated and tested in a healthcare Information system to check its viability. The developed model was implemented iteratively until the users considered the algorithm fit for use. The data collection technique that was used in this study was interview questions that were to be answered from the literature review. The source of data for this study was secondary data source and the sampling method was non-probability sampling method. This involved purposive sampling as indicated on Table 2.5 which shows how the best algorithm was identified for further analysis in the study. The sample size in this study was 100 authors and 20 modern cryptographic algorithms that were identified in literature review, 5 out of 20 modern cryptographic algorithms were selected for further analysis in the study. The best performing modern cryptographic algorithm was selected to be compared with the developed cryptographic algorithm. The developed cryptographic algorithm was piloted in a health care facility by 2 senior security officers, 3 system administrators, 2 network administrators, 1 nurse, 2 doctors, 1 finance officer, 3 health information officers and 2 database administrators. The pilot study was conducted in a health information system and results indicated as shown in appendix 1. From the experiments and simulations AES was found fit for comparison with the developed cryptographic algorithm with base 64 512 bits.

Figure 3.1 illustrates how design research methodology relates to the design, development, testing, piloting and deployment of the cryptographic algorithm base 64 512 bits. Stage 1 shows problem identification and motivation which relates to the study of existing modern security frameworks. Stage 2 relates objective of a solution to study of how security algorithms have been implemented and analysis of the existing modern cryptographic algorithms. Stage 3 shows how design and development relates to the development of the prototype or model. Stage 4 and 5 demonstrates evaluation and testing of the model. This

ensured that the empirical evidence was obtained during evaluation phase of the developed algorithm. The last stage , 8 indicates communication which relates to the results of the study and conclusion.

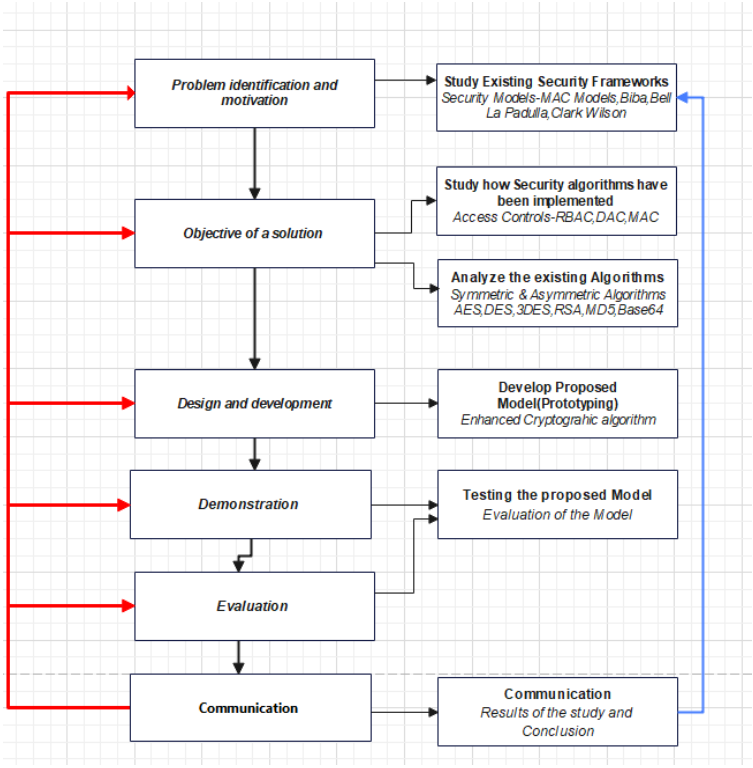


Figure 3.1 Design Research Methodology

3.2 Cryptographic Algorithm Base64 512 bits Development

This section describes how the model was developed from requirement gathering and analysis to design, testing and analysis of test results. The artifact was designed and developed from the analysis of the security features and characteristics of the existing cryptographic algorithms obtained from literature review.

3.2.1 Requirements Analysis and Data Classification

Requirements for artifact development were obtained from literature review. The requirements for system development was obtained from the analysis of the results from

evaluation criteria of the main characteristics and features of an acceptable cryptographic algorithm.The cryptographic algorithm that was found to meet the criteria was selected and the features that did not meet the criteria were improved to develop a cryptographic algorithm Base64 512 bits at the data level. AES cryptographic algorithm was identified and fixed key length of 512 bits was added unto the algorithm to improve on data protection at the data level.

The features and characteristics of existing cryptographic algorithms that were incorporated for artifact development were as shown in figure 2.4. Strength on brute force attack, known plain text vulnerability, use of private Key, Ease of data decryption and Database performance, Role Based Access Controls. The evaluation and analysis of the features and characteristics of the existing cryptographic algorithms that were obtained as the input requirements for the artifact development were classified as indicated in Table 2.5.

3.2.2 Design Phase

The requirements gathered during requirement gathering phase were incorporated to design a model that was used for development of the cryptographic algorithm Base64 512.The design of the artifact was based on design modelling tools such as the use case diagrams, sequence diagrams and a class diagram for the database structure. This phase involved description of a component diagram from the use case diagram and the algorithm data flow diagram was used to display the implementation of the prototype.

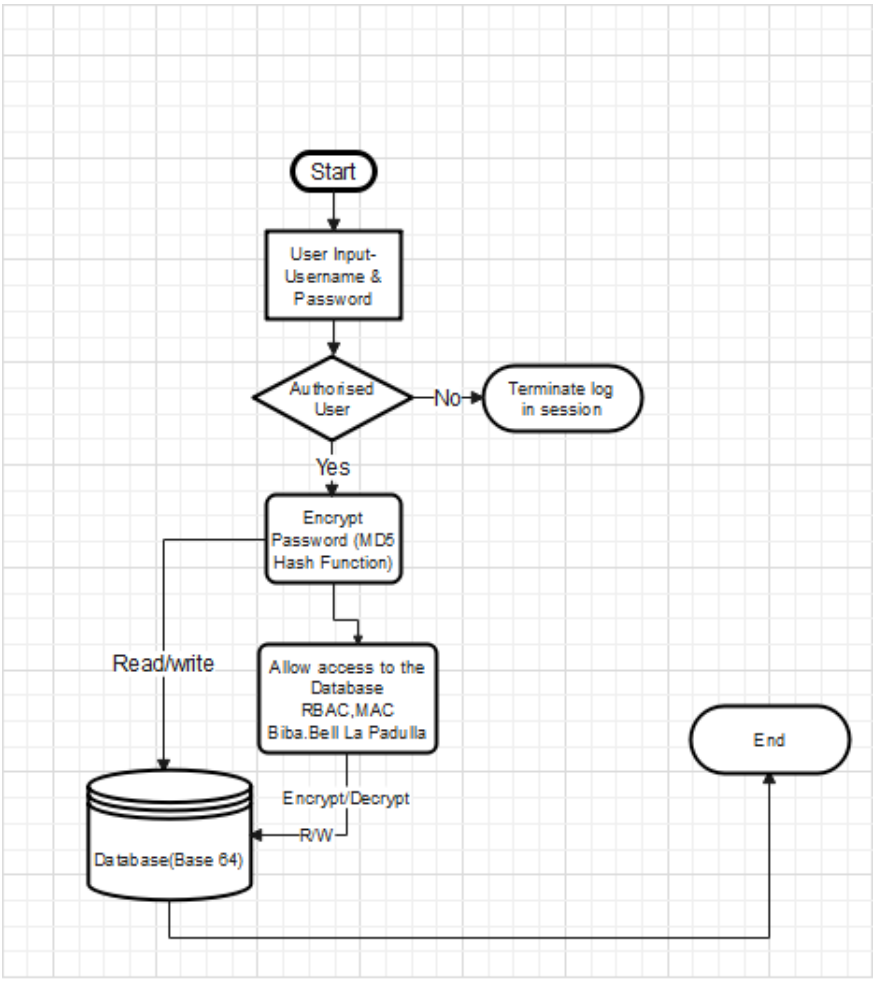


Figure 3.2 Data Flow Diagram

Figure 3.2 demonstrates a Data Flow Diagram (DFD) that shows the flow of data from input, process and output. The figure shows one example of DFD of a user login activity.The user input username and password and the login details are autheticated depending on the roles and permissions assigned to the user. The password is encrypted, read and write functions are performed using RBAC and MAC frameworks and stored in the database.

3.3 Development Phase

Development of the artifact was done using Python programming language with Django framework and involved integration of the following data level security measures as illustrated on Table 2.5, Role Based Control Access, brute force attack, known plain text vulnerability, private key, ease of decryption and database performance. Each of the security measure was implemented at different levels and stages as illustrated in Figure 3.3. The figure demonstrates user access levels and security control measures. It shows two users, one is authorized user and the other is unauthorized user. The user is authenticated before access to the application and further unto the database. The data is encrypted and stored in the database and can also be retrieved when needed. To ensure authentication of users, roles, password profiles and access to the database, a Role Based Access Control security measure was implemented. This security measure involved restriction of users and applications from accessing the database thus a user could only access the database according to the roles and permissions assigned to them and according to the verification of their passwords. MAC security models: Biba and La Padulla security measures were added to RBAC to control the extent to which read and write actions could be executed by a user or an application(Lee et al., 2020b). To enhance the strength on brute force attack MD5 hashing function encryption algorithm was used to mask passwords permanently(Ed Oswald, 2022). The password policy was to ensure that all the parameters set by a user to access the system would comply with the policy. Thus, any attempt by an unauthorized user to guess the password would be impossible. Advanced Encryption Standard, Base64 Algorithm, 512 key length bits was used for encryption and decryption of data stored at the database and this was to improve known plain text vulnerability. Combination of AES and Base64 algorithm with an additional of 512 bits at the data level made it very difficult for any malicious attacker whatsoever to guess the plain text that was encrypted to cipher text.

Delay in data retrieval can lead to death and Medical legal penalties thus ease of data decryption and database performance as a security measure, database optimization was automatically configured for each row, column, table and views. This ensured that the speed of data decryption was fast to allow for ease of access to data at the data level when necessary. Figure 3.3 illustrates how the architecture or the model of the cryptographic algorithm with base 64 512 bits was designed and developed. The figure shows the 5 major identified security measures corresponding to specific security database approaches, security models and cryptographic algorithm methods. RBAC and MAC were applied at application level and database level respectively. Brute force attack, known plain text vulnerability and ease of decryption was used for encryption and decryption of stored data in the database.

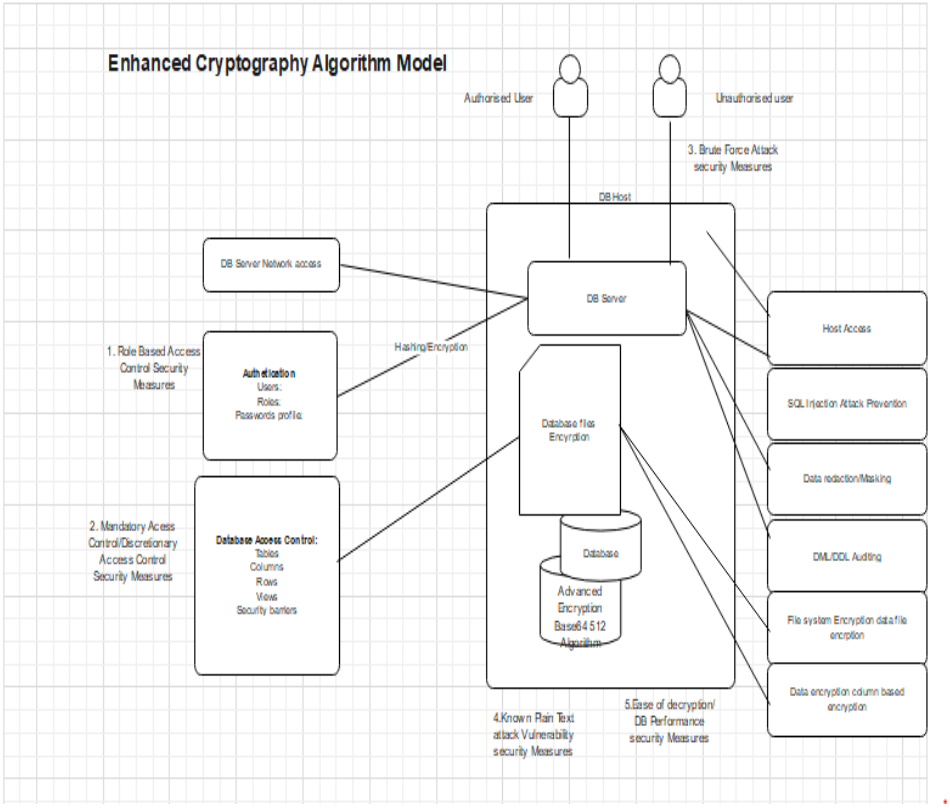


Figure 3.3. Cryptographic Algorithm Model

Figure 3.3 illustrates development of the prototype, modelling tools such as Entity Relationship Diagrams(ERD) ,Data Flow Diagrams (DFD) and class diagrams were used to ensure the quality of the prototype.Entity Relationship Diagram described the relationship between the entities while Data Flow Diagram described the flow of data. It defined the expected input and output for the process of encryption and decryption of data at the data level.

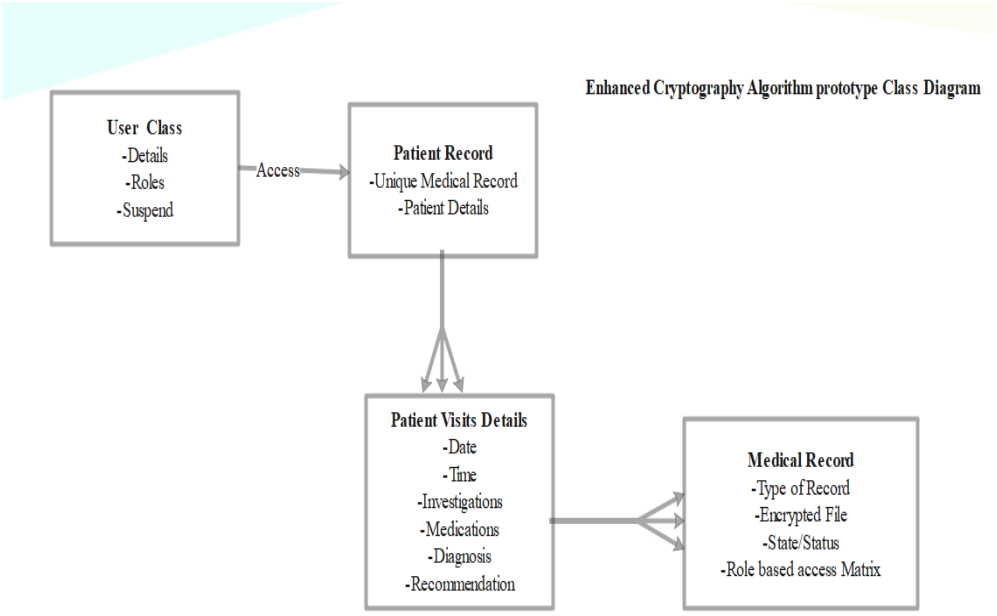


Figure 3.4 Class Diagram

Figure 3.4 illustrates a Class Diagram of the developed cryptographic algorithm which describes how a user class accesses patient record in relation to patient visit details and medical record. The respective specific security controls were implemented at the application level and database level as shown. In Figure 3.4 RBAC and MAC was considered in the class diagram to manage access levels using role based access matrix

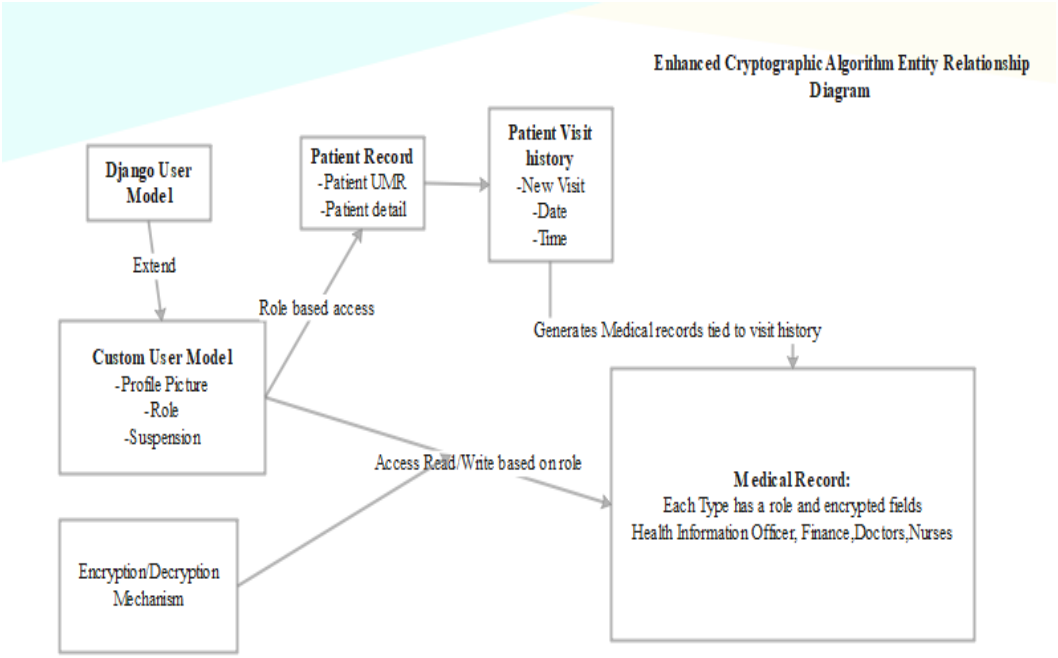


Figure 3.5 Entity Relationship Diagram

Figure 3.5 illustrates Entity Relationship Diagram (ERD) in the design and development of cryptographic algorithm base 64 512 bits. The figure shows how different entities relate to each other and how each security measure is considered in the development of cryptographic algorithm with base 64 512 bits.

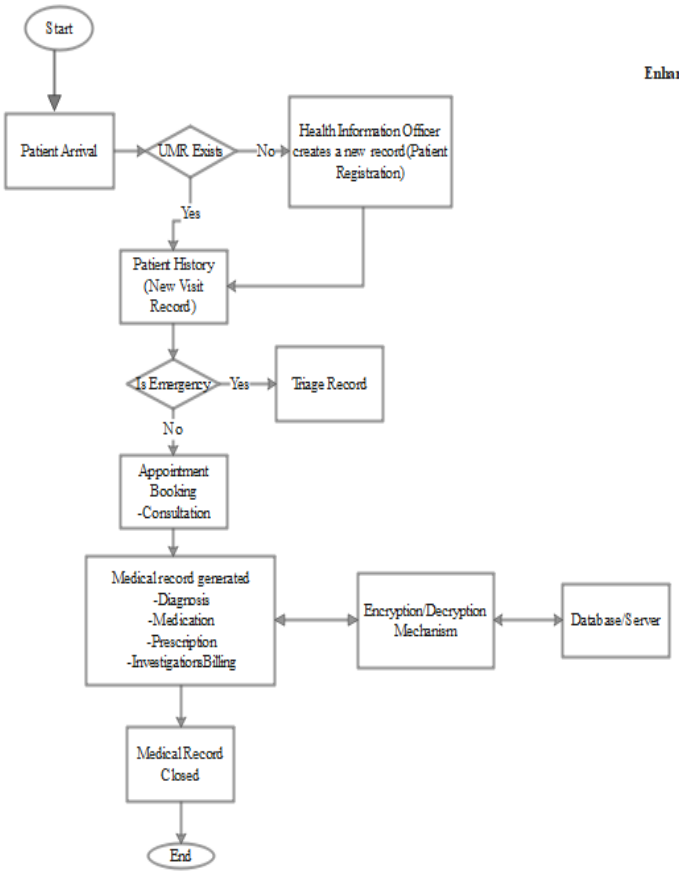


Figure 3.6 Data Flow Diagram

Figure 3.6 shows a data flow diagram that demonstrates how data flows from the application to the database level. Different security measures are implemented at specific stages during flow of data. An example of a security feature on the DFD is encryption and decryption mechanism stage during storage and retrieval of data.

3.3.1 Base64 512 bits Cryptographic Algorithm Pseudocode

The main objective of the pseudocode was to ease the development of the source code for development of the algorithm. It was used as a sketch code to help in the development of the algorithm and to reduce errors and bugs during the development phase. The use of pseudocode in the development of the algorithm before real coding reduced the amount of time that was required to complete the development.

BEGIN the program

ENTER Username and Password

IF Correct username and Password

<User logins>

ELSE Wrong Username and Password Contact System Administrator

ADD Record

<Create record and encrypt>

REPEAT To create and encrypt different records

DISPLAY To decrypt and view the records saved into the database

END

3.3.2 Testing the Prototype

The artifact was tested and piloted in a healthcare information system through experiments and simulations by 2 senior security officers, 3 system administrators, 2 network administrators, 1 nurse, 2 doctors, 1 finance officer, 3 health information officers and 2 database administrators. The involvement of systems security experts and simulations in the testing of the prototype ensured the quality of the model since every area of the application and database processes was tested appropriately and accurately in the following steps:

Step 1: Role Based Access Control Security measure

This test case was conducted by experienced system security experts as indicated in appendix 2 to ascertain that users and applications with specific roles and permissions were

authorized to access specific data in the Database. This was the first security measure to be tested as it was the initial point to begin the test case for all the scenarios. The quality of this security measure was tested to ensure that an unauthorized users and applications could not access the database and also to ensure that only authorized users with the authorized roles and permissions could access the application and the database. Different users with specific roles and permissions were created for testing purposes. These roles were for Database Administrators, System Administrators, System Security Administrators, Health Information Officers, Nurses, Doctors and a Finance Officers. These roles were assigned at different access levels to control access to the database and the application. The results and observation of each role and user were recorded for reference and further analysis.

Step 2: Strength on Brute Force Attack Security Measure

To test this scenario System Security experts tested several password rules and controls to test the strength of the algorithm on brute force attack. To test the strength of the prototype on brute force attack, several attempts of wrong passwords and usernames were tested. To pass this test the wrong or guess passwords was not to allow access to the application and to the database. The strength on brute force attack was significant as the access to the application and to the database could not succeed since the passwords and the usernames were hashed and masked completely before saving them in the database. This ensured that no guess or wrong passwords could allow access to the application or the database. These results were recorded for further analysis in the study.

Step 3: Known Plain Text Attack Vulnerability

In this step the prototype was tested by Database Administrators and a System Security experts for Known Plain Text Attack Vulnerability as a security measure. In this scenario any small change in plaintext was tested to find out if it would produce a significant change in the cipher text. In the first scenario, a plain text was slightly changed to test whether a significant change would be observed in cipher text but since in the development of the artifact alerts for notification were configured to notify the relevant users of any data change or attack, the respective users were notified. In addition to alerts and notifications the Avalanche affect was calculated to find out if a change in one bit of plain text could result to a change in many bits of the cipher text. After several tests, the experiments showed an average of 55% Avalanche effect, meaning that the developed cryptographic algorithm Base64 512 bits was strong in data security at the data level as compared to the modern existing cryptographic algorithms. The results of this test case were recorded for further analysis during the study.

Step 4: Ease of Decryption and Database Performance

In this scenario a test patient was set up and the bio data of the patient which involved patient registration data and patient medical records which include patient history, complaints, investigations diagnosis, medications and vitals entry was encrypted and saved in the database. To test the speed of encryption and decryption, that is the amount of time taken to encrypt plain text into cipher text and the amount of time taken to decrypt cipher text into plain text for storage and retrieval of data in the database A timer was set to test how much time it would take to decrypt and encrypt and vice versa. This test case was conducted by a Database Administrator so as to measure the performance of the database in terms of CPU utilization and Memory consumption as the encryption and decryption of

data was being performed. The results of these scenarios were recorded for further analysis in the study

3.4 Test Analysis

This section describes how the test analysis was conducted. During the testing phase of the prototype, four scenarios were tested representing the main security measures that were identified in the study. The main security measures that were tested and analyzed were as follows:

3.4.1 Role Based Access Control Test Case

To test the roles and access controls, different roles with permissions was created and assigned to different users. Each user was assigned a role based on the access control to test actions at the database. The role could either Create, Read, Update and Delete records at the database. A combination of the CRUD actions was also tested to analyze the access control at the data level. RBAC is the most flexible form of access control and has promised alternative to traditional discretionary and mandatory access controls.(Soe & Phyu, n.d.) In this study, RBAC was implemented in the development of the artifact with three entities,users, roles and permissions.To test this scenario different users were created with different roles and permissions. The identified CRUD scenarios were identified and tested for RBAC. The results of the tests showed that the security of the system was as good as its RBAC measures.The strength of the system roles and permissions indicated an improved access control to the objects at the database.The results of the analysis were recorded for consideration in further development of the Cryptographic algorithm with Base64 512 bits.This was to ensure maxmum security in the control of access to the database. Only specific users, user groups and applications could access specific levels of a database without gaining access to the rest of the database. This was necessary because

in a healthcare information system some data is more sensitive than others.(George & Bhila, 2019b) For example patient registration details and electronic medical records are very sensitive and must be kept confidential.(The Protection of Personal Data in Health Information Systems-Principles and Processes for Public Health, n.d.) RBAC in this study was incorporated with Bell LaPadula (read down and write up rules) and MAC policies. These enhanced the security of the artifact as compared to Modified Hill cipher which was found to have no RBAC policy as indicated in testing the prototype Step 1. The criteria to score this test case was set with creation of a user ID which was mapped to a role ID and permission ID mapped to a role.This was repeatedly performed for specific users,roles and permissions and the database actions noted. It was observed that the incorporation of RBAC policy as a control access to the database enhanced data level protection at the the database as compared to the modern existing cryptographic Algorithms which did not incorporate any form of access control.

Table 3.1. MAC Data classification Levels

Level	Description	Range
VS	Very Sensitive	30-39
S	Sensitive	20-29
C	Confidential	10-19
U	Unclassified	0-9

Table 3.1 shows four classification levels of MAC data with there corresponding ranges and description. The MAC data is considered to be very sensitive if it ranges between 30-39 units according to MAC data classification.(Dollinger robert, 2022)

Table 3.2. Database Objects

Object Name	Level
System Administrators	39
System Security Administrators	39
Database Administrators	39
Doctors	38
Nurses	38
Health Information Officers	38
Finance Officers	29

Table 3.2 shows the database objects used in the development and configuration of cryptographic algorthm Base64 512 bits. Each specific user was assigned the level corresponding to MAC level in the design of data sensitivity.

Table 3.3 Sample Permissions

Permission ID	Permission Name	Object	Access Rights
1	Read Investigations	Doctor	READ
2	Write Investigations	Doctor	WRITE
3	Read Complaints	Doctor	READ
4	Write Complaints	Doctor	WRITE
5	Read Patient	Health Information Officer	READ
6	Write patient	Health Information Officer	WRITE

Table 3.3 shows sample permissions with permission name, the object and the access rights. The access right determined the object that would be assigned a corresponding permission.

Table 3.4. Sample Roles

Role ID	Role Name	Level
1	System Security Administrator	39
2	Database Administrator	39
3	System Administrator	39
4	Doctor	38
5	Nurse	38
6	Health Information Officer	37
7	Finance Officer	33

Table 3.4 illustrates the roles of users and the corresponding MAC levels for each role. This was to ensure that each role had access to data sensitivity according to MAC levels.

3.4.2 Strength on Brute Force Attack Test Case

In this test analysis scenario, the following were tested for password policy: the length of the password was to be at least more than 8 characters, a combination of letters, numbers and symbols, restrictions on use of a person's name, any three wrong attempts to the account to require the administrator to unlock, progressive delay to lockout the account for a limited amount of time after failed login attempt. Each failed attempt made the delay longer, Captcha to allow users to perform simple tasks to login a system, multi factor authentication to authenticate identity and access to accounts, enforcement of periodic password change. The password and username were hashed and saved to the database. The results of this experiment guided on the development of Cryptographic algorithm with Base64 512 bits. To test the strength of the developed artifact against brute force attack

vulnerability, THC Hydra tool was used to identify vulnerabilities in the database. Brute force attack is a simple attack method and has high success rate (Imperva, 2021). While some attackers may still perform brute force attacks manually today almost all brute force attacks are performed by bots (Imperva, 2021).

3.4.3 Known Plain Text Attack Vulnerability Test Case

In this test analysis, the prototype was tested for known plain text Vulnerability. The plain text was generated and a mathematical calculation for algorithm was subjected to it to generate a cipher text. The plain text was subjected to different key lengths of data to test if the plain text could be easily guessed. The results of this test analysis showed that the longer the Key length the harder it was to guess the plain text. The artifact was developed using AES and Base64 Algorithm with fixed key length of 512-bit key size to ensure that the combinations used to encrypt the plain text into cipher text could not be easily predictable. This was compared with the results obtained from the existing algorithms which showed that the cryptographic algorithm Base64 512 bits had a higher entropy of 55% as compared to the existing modified hill cipher algorithm that showed 53%. Security of an algorithm is measured by computing number of decryption steps, the higher the number of decryption steps to decrypt the ciphertext to get original message shows higher level of security. (Charru, 2014). This experiment showed that the cryptographic algorithm Base64 512 bits had a low risk vulnerability to plain text attack as compared to other existing cryptographic algorithms.

3.4.4 Ease of Decryption and Database Performance Test Case

In this test analysis scenario, the prototype was tested for database performance during encryption and decryption. Different sizes of data were tested for encryption and decryption processes and the turnaround time recorded. Since cryptography is the science

of protection of private information from unauthorized access, ensuring data integrity, authentication, and other tasks, it incorporates the principles and methods of transforming plaintext into ciphertext and then re-transforming that message back to its original form (AMedina, 2019). The prototype was developed with data encryption and decryption functions to help secure sensitive information and to provide confidentiality to private data, indexing and hashing capability functions were configured at the data level for quicker retrieval of data. After a series of tests, it was observed that the cryptographic algorithm Base64 512 bits performed decryption faster as compared to the existing algorithms. For a healthcare information system, speed in data retrieval is very critical because a delay in data retrieval can be fatal as it can cause death or delayed patient care.

3.5 Deployment Phase

The cryptographic algorithm prototype was iteratively developed until it was deployed and validations were placed to keep the system user in check.

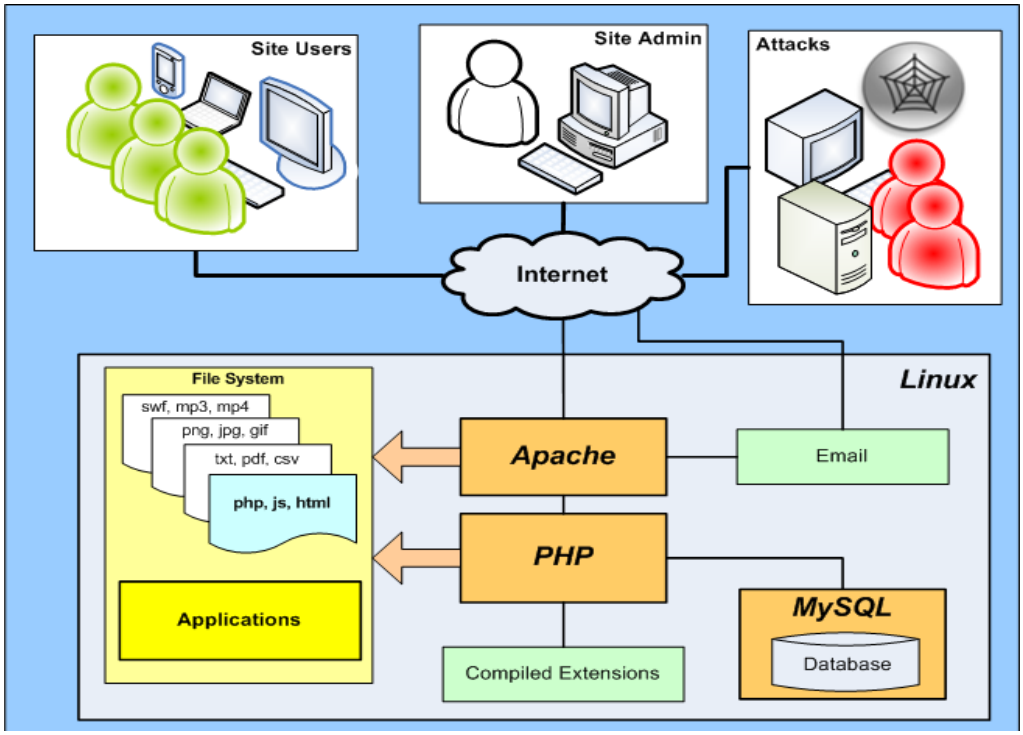


Figure 3.7 GitHub Deployment Framework

Figure 3.7 illustrates a GitHub deployment Framework that was used to deploy the developed cryptographic algorithm with 64 512 bits .Site users, site Admins and attackers were executed at the internet level to the apache and PHP for running the application and data stored in MySQL database.

CHAPTER FOUR

RESULTS

4.0 Introduction

This chapter contains a detailed discussion of the results of the research findings and detailed explanation of how each of the specific objective of the study was achieved.

4.1 Existing Data Encryption Algorithms in Healthcare Information Systems

The first objective of this study was to investigate the existing data encryption algorithms in Healthcare Information Systems and their security characteristics for data protection at the data level. An evaluation criterion was used to test the adequacy of each security feature for the selected cryptographic algorithm. From literature review 100 different authors were identified who described several modern existing cryptographic algorithms and only 4 modern cryptographic algorithms were identified for this study.

Table 4.1 Analysis on features and characteristics of the existing cryptographic algorithms

Algorithm	**Strength on brute force attack**	**Known Plain text Vulnerability**	**Use of Private Key**	**Database Performance (Ease of encryption and decryption)**	**Role Based Access Control**
Twofish	Strong	low	Yes	Slow	No
AES	Strong	Medium	Yes	Medium	No
TDES	Weak	High	Yes	Poor	No
DES	Very Weak	Very High	Yes	Very Poor	No

Table 4.1 illustrates the results of the first objective of the study which was to investigate the existing cryptographic algorithms. Twofish, AES, TDES and DES were selected for investigation and their major security features and characteristics analyzed. From the

results AES was selected for the next phase in the study. It was strong on brute force attack, medium known plain text vulnerability, use of private key and medium speed on database performance. On the other hand, all the other algorithms lacked RBAC security feature. AES algorithm was improved by addition of fixed key length of 512 bits and RBAC to develop cryptographic algorithm with Base64 512 bits.

4.2 Data Protection Techniques in Healthcare Information Systems at the Data Level.

The second objective of the study was to evaluate data protection techniques in Healthcare Information Systems at the data level for integration in the design of the cryptographic algorithm with Base64 512 bits. Table 4.2 shows the analysis of the major data protection techniques as they were obtained from literature review: Authentication Based security, Trust based security, cryptographic based models and access control security models. Analysis for the identified data protection techniques was conducted and the results recorded as shown on Table 4.2.

Table 4.2 Evaluation and Analysis of Data protection Techniques

Data Protection Technique	Author/Year	Number of papers	Security strengths based on widely applied security metrics.	Analysis/Discussion	Remarks
Authentication Security Models	Security and Usability in Knowledge-based User Authentication: A Review George Samaras, Marios Belk Department of Computer Science, University of Cyprus CY-1678 Nicosia, Cyprus cssamara@cs.ucy.ac.cy Christina Katsini, Christos Fidas, Nikolaos Avouris, Department of Electrical and Computer Engineering, University of Patras 26504 Rio, Greece katsinic@upnet.gr 2016	5	Uses Password, Biometrics and PIN for user authentication.	Authentication Security models are the most preferred data protection techniques. They provide a variety of options for data protection either as text, Pin and graphical based. The strength and the length of the password can be predetermined to enhance the security. Authentication security models lie under three major categories-Knowledge based (passwords), token based (credit cards) and biometric based (fingerprints)	Authentication Security Model is preferred in this study as Knowledge-based authentication is currently the most common approach for gaining access control.
Trust based Security	A survey on IoT trust model frameworks Davide Ferraris1 · Carmen Fernandez-Gago1 · Rodrigo Roman1 · Javier Lopez1 October 2023	7	Trust Management, metrics, models (Trust Management Framework)	Trust is strictly dependent on the actors involved in a trust interaction. Typically, there are two entities (at least) involved in a trust interaction, one is the trustor (the entity which places trust) and the other one is the trustee (the entity in which trust is placed)	Trust based security model was considered in this study since in order to integrate trust security models in any system it is strongly recommended to consider it within trust management framework

Access control-based security	A systematic literature review for authorization and access control: definitions, strategies and models Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer and Josef Küng	8	Authorization table, ACL, RBAC, Capability List, Biba, Bell La Padulla, Clark–Wilson, (OrBAC), VBAC	Authorization table used in database management systems, Access control list (ACL) the most common and basic form of access control for limiting access to data on shared systems Capability list the conceptual approach similar to ACL, but with the access matrix stored by row (i.e. subject view). Access control by roles that ensures system activities and resource permissions are associated to some defined role(s) rather than assigned directly to users Organization-based access control (OrBAC) has evolved because of the need to structure a given organization into sub-organizations and specify their different authorization policies within one framework View-based access control (VBAC). This is a virtual table having rows and columns defined by a query based on the database tables, but without physical storage	Access Control based Security was preferred for integration in this study for its ability to restrict access from all identifiable access areas. This enhances authentication and system administration.
Cryptographic Based Models	Cryptography based Techniques of Encryption for Security of Data in Cloud Computing Paradigm. Adel Rajab1, Sehrish Aqeel2 , Mana Saleh Al Reshan1 , Awais Ashraf 3 , Sultan Almakdi1 and Khairan Rajab1 2021	10	Asymmetric key cryptography, Symmetric key cryptography, Hash function cryptography, Advanced Encryption Standard (AES), SHA-512 is a hashing function algorithm, DES, 3DES, IDEA, RSA, ECC, Homomorphic and Blowfish	Secure keys are crucial to protecting data at the data level. The advancement of encryption is moving towards an inevitable destiny of ceaseless sort of possible results. Although hacking is unstoppable cryptographic algorithms can enhance data protection	This model was most preferred for this study as SHA-512 hashing function algorithm that takes 64 bytes or 128 bytes of data for the encryption and decryption process, and digest sizes are 224, 256, or 384 bits. SHA-512 takes 64 or 80 rounds to convert the plain text into ciphertext.

The results of the analysis as indicated in Table 4.2 on the remarks column shows that four identified data protection techniques were considered for progression on the next phase of design and development of the cryptographic algorithm with base64 512 bits. Authentication based security was analyzed for authentication of users and applications into the database. Authentication method was instantiated to different applications and different users for validation. Users and applications were authenticated into the system using their specific user IDs, application IDs and passwords. The results showed that adequate implementation of authentication methods improved security at the database level. The analysis of Trust based security technique was obtained from vigorous testing of trust-based security methods into the system. This was done by testing to ensure that the users and applications performed the functions that they were designed to perform. When a user or application was subjected to unmatched function it would fail. Access control-based security analysis was conducted by designing roles, permissions, users and access controls to the database. Different users and applications were assigned different roles to perform specific actions in the system. Database actions (CRUD) create, read, update and delete were performed to ascertain that specific users with specific roles could only access and perform specific actions. The analysis of cryptographic security-based models was

conducted by testing of encryption and decryption of data of different sizes and the performance of the database. The second objective of this study was successfully obtained from the analysis of the identified main data protection techniques as shown on Table 4.2

4.3 Design and development of Cryptographic Algorithm with Base64 512 bits

The main and third objective of this study was to design a cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems. The cryptographic algorithm with base 64 512 bits was designed and developed using the results obtained from Table 4.1 and 4.2. Comparison on characteristics for data protection at the data level between modern existing cryptographic algorithm and the developed cryptographic algorithm with Base64 512 bits was conducted by simulation and experiments in a healthcare Information system. Table 4.3 shows test results and analysis from the comparison of the existing modern cryptographic algorithms and the developed cryptographic algorithm with base 64 512 bits.

Table 4.3. Test and Result Analysis

Algorithm	Encryption Time	Decryption Time	Memory Usage	Strength	Score
Base64 512 bits	0.00001729530560565185547	0.00001276421546930351	75.4453125	Very Strong	80%
AES	0.0000625309944152832	0.0000625309944152832	75.4453125	Strong	67%
Twofish	0.0000625309944152832	0.0000625309944152832	75.4453125	Medium	50%
TDES	0.000001093387603759 7657	0.0000010933876037597657	75.4453125	Weak	42%
DES	0.000001093387603759 7657	0.0000010933876037597657	75.4453125	Very Weak	22%

From the evaluation of the algorithms as shown on Table 4.3 the research results show that the developed algorithm with Base64 512 bits scored a highest score 82% on overall performance. This empirical evidence was obtained from the evaluation of the algorithms on their performance on all main security features and charateristics.

4.3.1 Model Development

The cryptographic algorithm with Base64 512 bits model was developed using Python programming language and Django Framework as shown in *Appendix 1*. This model was used in the development of the cryptographic algorithm. In the development of this model both functional and nonfunctional requirements were considered. Figure 4.1 displays a Django administration dashboard for the development and management of the base 64 512 cryptographic algorithm.

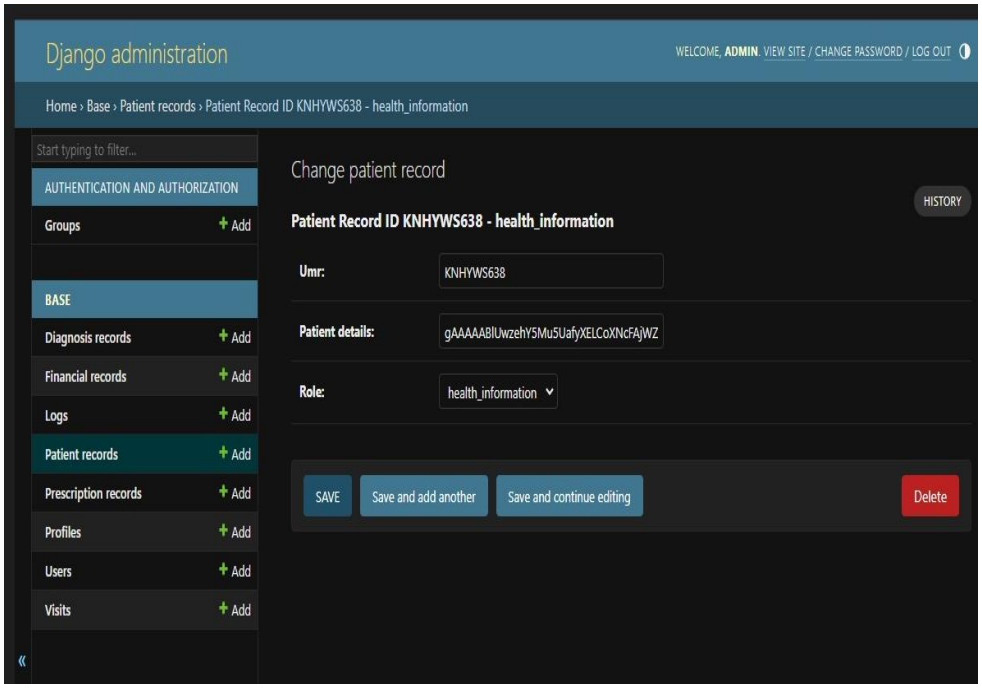


Figure 4.1 Django Administration

4.3.2 Functional Requirements

Functional requirements were the mandatory requirements for the development of the cryptographic algorithm Base64 512 bits model that defined what the algorithm must do and what its functions and features are. The functional requirements for the development of the cryptographic algorithm were obtained from the literature review as described in *Figure 3.3. Cryptography Algorithm Model*. The key features and functions of the cryptographic algorithm with Base64 512 bits model were, use of Role Based Access Control policy to control access of subjects(users) and their actions at the database level. This ensured authentication of users before access to the database and also to control access to different database levels. The main function of a good cryptographic algorithm is to ensure that no unauthorized users or malicious authorized users can access the database. The developed cryptographic algorithm with Base64 512-bit model was developed with RBAC, MAC, security models such as Biba, Bell La Padulla and Clark Wilson for read down and write up policy as indicated on *Table 4.2*. For improved data level protection,

the development of the cryptographic algorithm with Base64 512 bits model included integration of AES algorithm, Base64 algorithm,512 fixed length key and MD5 algorithm. Integration of these techniques enhanced the strength on brute force attack, low risk for known plain text vulnerability and a secure private key. Automated database re-indexing technique was configured on the developed cryptographic algorithm model to improve on the speed of data retrieval during decryption for database performance. The results of the developed cryptographic algorithm with Base64 512 bits achieved this objective of the study by ensuring improved brute force attack. Guess of wrong password attempts could not penetrate the system and several use of wrong password locked out the user and sent a notification to the system administrator. The more the user failed logins the more it would delay the time to allow the user to lg into the system. Low risk on the known plaintext vulnerabilities was confirmed as it was observed that it was not possible to easily guess plain text from cipher text. The data that was encrypted could not be decrypted by unauthorized user. Higher database performance during encryption and decryption of data was observed from the developed cryptographic algorithm with Base64 512 bits. The database performed at an optimal speed during encryption and decryption of data. The database tables, columns, rows and views were automatically re-indexed to optimize database performance. These results were obtained from the various experiments and simulations performed in a healthcare information system.

4.3.3 Non-Functional Requirements

Non-functional requirements in the development of the cryptographic algorithm with Base64 512 bits were the requirements that described the general properties or features of the preferred cryptography algorithm. The following properties were incorporated in the development of the cryptographic algorithm with Base64 512 bits: scalability, portability, performance, speed, availability and maintenance. To ensure that the developed

cryptographic algorithm achieved scalability, SQL Lite DB was used to simplify deployment to different Database and support different users. To develop the cryptographic algorithm that would overcome the slow speed of data encryption and decryption and to enhance the speed of the database performance, an automated re-indexing function was implemented at the data levels including tables, rows, columns and views. This ensured that the developed cryptographic algorithm was easy to maintain and update. The development of the cryptographic algorithm with the specification of the non-functional requirements ensured that the algorithm met all the criteria for a preferred cryptographic algorithm from literature review as described in *Figure 2.4. A Model for evaluation criteria of an acceptable enhanced cryptographic algorithm*. The results of this experiment and simulation was obtained in a healthcare information system.

4.3.4 System Design and Modelling

In order to ensure that the model that was developed was acceptable and met the main objective of the study, modelling tools such as ERDs, and DFDs were used in the development. The architecture of the developed cryptosystem was as illustrated in *Figure 4.2*.

Enhanced Cryptographic Algorithm System Design

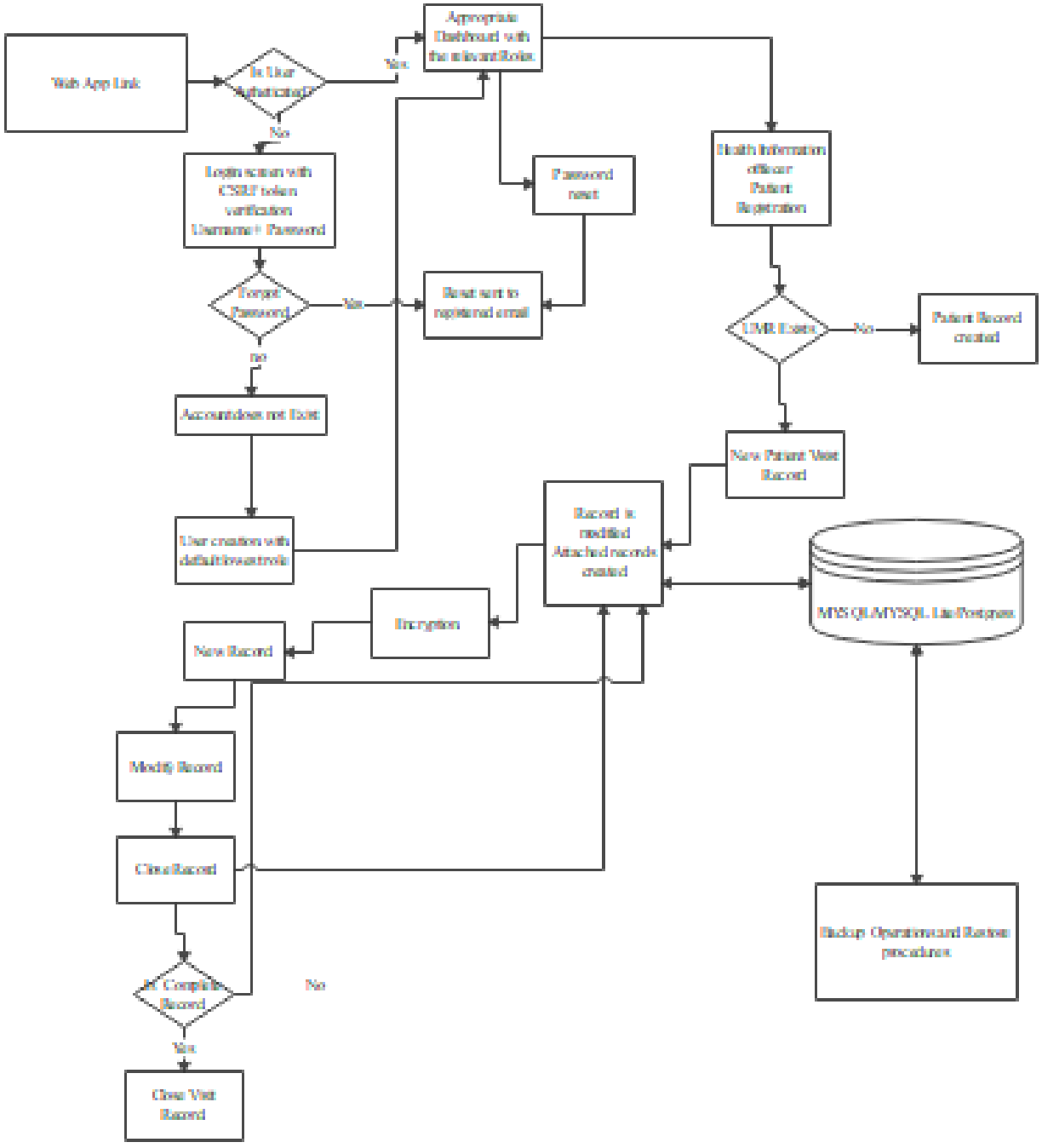


Figure 4.2 Base64 512 Algorithm Design

Figure 4.2 demonstrated how the actual system was to be developed by defining the technical specifications for both input and output parameters. Python programming language and Django framework were considered in cryptographic Algorithm with Base64 512 bits system design which were used to develop the cryptographic algorithm.

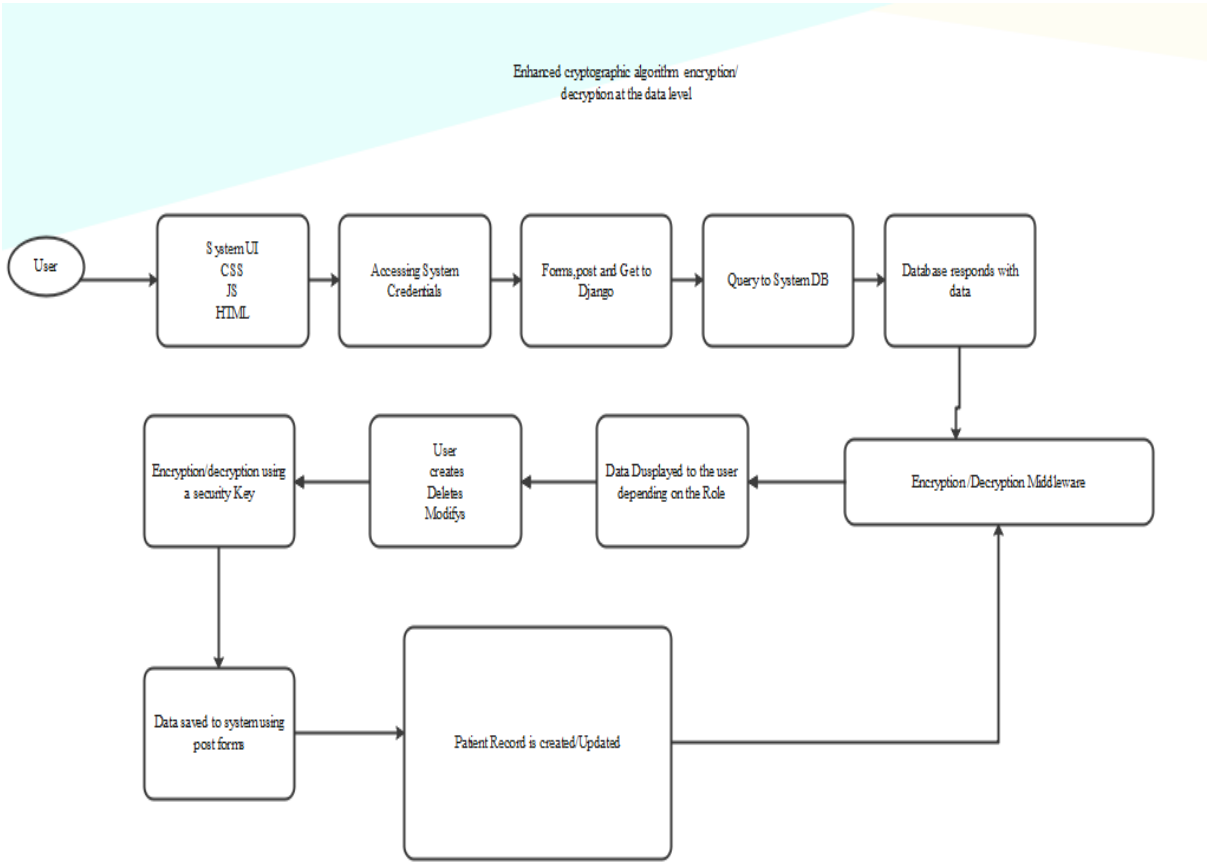


Figure 4.3 Encryption/decryption

Figure 4.3 illustrates how the system user interface was designed using CSS, JS and HTML to allow the users interact with the system. The users were to access the system with their credentials, forms, post and get to Django. This request sends a query to the database for validation and verification of the user's login details and a response is received from the

database with the status of the user. Encryption and decryption middleware perform either of the functions accordingly and the data is displayed to the user depending on the role matrix defined for each user as illustrated in *Figure 4.3 cryptographic algorithm; Encryption/decryption at the data level.*

The results from the experiments and simulations in a healthcare information system for this scenario ascertained and showed that the main objective of this study was achieved which was to design an enhanced cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems.

4.3.5 Experiments and Simulations

The prototype that was designed and tested was a very key component in the development of the cryptographic algorithm with Base64 512 bits which was the main objective of this study. The testing of the developed cryptographic algorithm was conducted as experiments while other scenarios were performed as simulations. Two Senior systems security officers, three Database administrators and two system administrators were the key actors in conducting the experiments in the testing of the cryptographic algorithm with Base64 512 bits. The prototype was tested adequately and the results that were obtained were used to develop the cryptographic algorithm with Base64 512 bits.

Table 4.4 Summary of Test Results on specific objectives of the study

	Specific Objective	Findings	Key points of results achieved.	Meaning of the Results/Findings	References
1.	To investigate the existing data encryption algorithms in Healthcare Information Systems and evaluate their security characteristics for data protection at the data level	**Data encryption algorithms** 1.Symmetrical 2. Asymmetrical **Major Security Characteristics** 1.Role Based Access Controls 2. Strength on brute force attack 3. Known plain text vulnerability 4. Use of private key 5.Ease of encryption and decryption (Database Performance)	Use of private key with AES of 512 bits strengthens the major security characteristics of data protection at the data level. Addition of an encryption layer using Base64 algorithm at the database level reduces data breach in a healthcare information system	A preferred cryptographic algorithm should meet the minimum criteria of the major security characteristics as demonstrated on the criteria for selection on *table 2.2*	According to Paragas J, Sison A, Medina R2019 IEEE 11th International Conference on Communication Software and Networks, ICCSN… The author explained that manipulation of mathematical calculations can enhance the security of an algorithm.
2.	To evaluate data protection techniques in Healthcare Information Systems at the data level for integration in the design of the cryptographic algorithm with Base64 512 bits	**Data protection techniques in healthcare information systems at the data level** 1. Authentication based security 2. Trust based security 3. Access control-based security (DAC, MAC, RBAC) 4. Cryptographic based security Models	Use of security-based models in the design of cryptographic algorithms models facilitates the control of application and database access levels.	RBAC and MAC are the most preferred data protection techniques in healthcare information systems as these security-based models play a major role in protection of sensitive data.	According to Soe A, Phyu S MAC (Bell, La Padulla, Clark Watson) are used to control READ and WRITE actions in the database while RBAC are used to control roles, permissions, users and application access level to the database.

3.	To design an enhanced cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems	A cryptographic algorithm with Base64 512 bits model was designed as illustrated in *figure 3.3*	A cryptographic algorithm with Base64 512 bits model was designed, a prototype developed and tested through experiments and simulations in a healthcare information system.	Additional security layer of encryption using Base64 algorithm and use of AES with a fixed key length of 512 bits improved significantly the security of the sensitive data in a healthcare information system	The longer the fixed key length the harder it is to crack the algorithm. This is as a result of the several combinations that are used to generate the algorithm
4.	To evaluate the performance of the cryptographic algorithm with Base64 512 bits in protecting data on healthcare systems	The speed of encryption and decryption of data was evaluated through a series of simulations in a healthcare information system. Different size of data was encrypted and decrypted and the turnaround time recorded for several scenarios to obtain the best performing time index.	Re-indexing of the healthcare information system database was automatically configured for improved database optimization and performance with no human intervention.	Delay in Patient data retrieval when it is required is fatal and also attracts medical legal issues. A good healthcare information system must therefore provide encryption of data very fast for data privacy and confidentiality and on the other the decryption of the secured data must be easy to retrieve when needed.	According to Data Protection Act 2019, Kenyan citizens have rights for data protection and thus all patient's data must remain confidential and private in a healthcare information system.

As it is indicated on Table 4.2, each cryptographic algorithm has got its own individual strength and weakness and thus the developed Cryptographic algorithm with Base64 512 bits was evaluated for the following major security characteristics, known plain text attack Vulnerability, Role Based Access Control, strength on brute force attack, use of private key, ease of decryption and database performance. The results obtained from each parameter and scenario was compared to modern existing cryptographic Algorithm as was identified from the literature review. As illustrated on *Table 4.3*, the developed

cryptographic algorithm with Base64 512 bit had a lower risk for known plain text attack vulnerability as compared to the modern existing cryptographic algorithms which had a significant high risk for known plain text attack vulnerability. The encryption, decryption mechanisms, database security approaches and security models such as Role Based Access Controls ensured that the plain text could not easily be manipulated in case of an attack. In a healthcare information system, the data stored in the database is very sensitive and critical and therefore it must be protected from any data leakage from both malicious authorized users and unauthorized users. The algorithm should have a very low risk of known plain text vulnerability as it was demonstrated on the results of the experiments and simulations. Role Based Access Control was also tested to ensure that specific users and applications had specific roles and permissions assigned to them to write/read data in the database. This security measure ensures protection of data at the data level by validating and verifying the users and applications before they can access the database. During this experiment the password policies and access controls were tested to ensure that the usernames and the passwords were encrypted before saving in the database using hashing function which is irreversible. All identified existing cryptographic algorithms lacked RBAC mechanism thus the risk was very high for this security parameter as compared to the developed cryptographic algorithm with Base64 512 bits. The scenarios tested the verification process when a new user was to be created in the system when the account of the user did not exist. Strength on brute force attack as a security measure was experimented to test the strength on brute force attack of the developed cryptographic algorithm. This scenario was to test the behavior of the developed cryptographic algorithm with Base64 512 bits in the event that an attacker guessed several passwords using certain techniques to crack and penetrate onto the system. This was implemented on the developed algorithm by enforcing strong password security policies and controls that made it very difficult for anyone to easily guess

the password. For example, use of one's name as the password, date of birth, email address, family names, use of less than 8 characters, mixture of numbers, letters, alphanumeric, small and capital letters including the configuration of the password to expire after a certain period of time. The developed cryptographic algorithm was tested for database performance during encryption and decryption process. A preferred cryptographic algorithm should not compromise the performance of the database during retrieval of data from the database or during encryption of data for storage in the database. A fast database is desirable in a healthcare information system as the patient data is very critical and must be available to a patient as soon as it is required. A delay in retrieval of patient data can easily cause complications, death and further medical legal cases. Therefore, in this scenario simulations to test the amount of time taken to encrypt the data, time taken for the data to be saved in the database, the time taken to decrypt the data from the database was performed and the results recorded including the generated turnaround time for different scenarios which involved the amount of data encrypted and decrypted and the time taken for each case. The type of data to be decrypted and encrypted was tested also and the amount of time taken for each scenario recorded. The overall results of the experiments and simulations showed that an additional layer of security using Base64 and AES of fixed key length of 512 bits at the data level and automation of database optimization improved the overall performance of the database.

4.3.6 Validity Test

Thematic analysis was used to test the validity of the developed cryptographic algorithm in comparison with the modern cryptographic algorithms during experiments and simulations. Thematic analysis was the best analysis approach in this study to test the validity of the developed algorithm since the main objective of the study was to design and implement cryptographic algorithm with Base64 512 bits to enhance data protection in

Healthcare Information Systems. The six thematic analysis steps (Familiarization, coding, generating themes, reviewing themes, defining and naming themes) were followed to achieve data level security effect as the themes to define the validity of the developed algorithm during experiment and simulation. The five comparison parameters which were identified as the major cryptographic characteristics were tested in a web application for the selected existing cryptographic algorithms and cryptographic algorithm with Base64 512 bits respectively. This was done iteratively with different scenarios until the desired results were achieved.

Thematic Analysis

The security features and charateristics of each cryptographic algorithm were tested and the results compared between the developed cryptographic algorithm and the selected modern existing algorithm using thematic latent approach. The additional security layer built on Base64 algorithm with fixed key length of 512 bits and AES encryption algorithm adversely reduced the risk for the known plain text vulnerability, improved strength on brute force attack, and use of security models such as RBAC enhanced data level security as each role and each user had specific access levels to the database. The results of the experiments and simulations showed that the developed cryptographic algorithm with Base64 512 bits had a very low risk vulnerability at the data level as compared to AES algorithm.

4.4 Performance Evaluation of Cryptographic Algorithm with Base64 512 bits

The fourth objective of this study was to evaluate the performance of the developed cryptographic algorithm with Base64 512 bits in protecting data in healthcare systems. This was compared with AES algorithm for evaluation and validation. The results of the comparison were the empirical evidence which showed that the developed algorithm

performed at optimal on data encryption and decryption. The developed cryptographic algorithm with Base64 512 obtained optimal database performance as compared to AES algorithm. To test the performance of the developed algorithm, various test scenarios were tested by Senior Database Administrators, Senior Security Officers and Systems Administrators. The analysis of the various scenarios on performance of the cryptographic algorithm with Base64 512 bits were as follows:

4.4.1 Encryption and Decryption Process

The senior security officers tested the viability of the algorithm to validate that the algorithm meets the characteristics of cryptographic algorithm. This process involved input of data into the system, various types of data using CRUD (create, read, update, delete functionality) and verifying the raw data in the database to be encrypted as the operations were being carried out. The encryption and decryption process implemented on the developed cryptographic algorithm with Base64 512 bits was found to meet encryption and decryption criteria as compared to AES algorithm which was observed to implement a very weak encryption and decryption.

4.4.2 Turn Around Time for encryption and decryption

In this scenario the system administrators tested the amount of time taken to encrypt and decrypt data during storage and retrieval processes. This was to measure the time delays for encryption and decryption- of data. A timer was set to calculate how much time it would take to encrypt data before it is stored in the database. The timer was set again to calculate the amount of time it would take to decrypt the data when retrieving the data for use. Different data sizes were obtained and tested for several scenarios. Small size of data was encrypted and decrypted and the speed of the database identified. A medium size of data was obtained, encrypted, decrypted and the speed of the database obtained. A larger data

size was encrypted and decrypted and subsequently the speed of the database obtained. The amount of time- taken for retrieval and storage of data at the database was obtained at every scenario. The overall observation was that Cryptographic Algorithm with Base64 512 bits performed at optimal speed for both storage and retrieval process and for all data sizes as compared to AES algorithm that was observed to slow database performance as the size of the data increased.

4.4.3 Strength on Brute force attack

The senior security officers in this scenario tested the strength of the Algorithm for brute force attack. Several attempts to gain access to the system through systematic guessing of password at login could not penetrate the database. This was because a robust password policy was implemented on the developed cryptographic algorithm with Base64 512 bits. To test the length of the password, the security officers would test different lengths of characters up to a minimum of eight characters. If the length was less than eight characters the test would fail and if the characters were more than eight characters the test would pass. To test the use of alphanumeric characters in a password the security officer would enter a mixture of numbers, digits and special characters. If any of the parameter was excluded into the password the test would fail otherwise if all the parameters were entered the test would pass. To test for password lock after a certain number of wrong attempts, the wrong password was entered the first time and the second time, this would give a warning that the account would be blocked if another wrong attempt was done. When the wrong password was entered the third time the account was blocked and access denied. To test restriction on use of names as a password, the system would check if the password contained a name similar to the username and if any similarity in the name was found the password would fail. The system timeout was also tested to ensure that if the user's screen was idle for a set time, the system would automatically lock the screen. The security officers tested this by

logging into the system and allowing the time set to lapse for session time out to occur. The results obtained from these tests indicated strengthened brute force attack at the data level for developed algorithm as compared to AES algorithm which was observed to be weak on brute force attack as the password policy was not implemented on AES algorithm.

4.4.4 Known Plain text Vulnerability

This scenario was conducted by a senior security officers to test the level of vulnerability for known plain text. A very small change in plain text resulted into a very huge change on the cipher text. Any alteration in plain text would send a notification immediately to DBAs and System Security officers for immediate action. Audit logs were also created to keep a record of the change using encrypted plain text and altering it as is, to see the change when the data is decrypted. Examining the Master logs for the record of changes. The developed algorithm had a very low vulnerability on known plain text as compared to AES algorithm which was observed to have a higher known plain text vulnerability. A small change on plain text did not result to any significant change on the cipher text.

4.4.5 Use of Private Key

Database Administrators conducted this test scenario to test the importance of the private key in the Algorithm and secure storage of the private Key. The DBAs confirmed that the private Key was stored securely and accessible to authorized users only. This private Key on the developed algorithm was stored in a different environment rather than the same environment where the system was running for private access only. The AES algorithm was observed to obtain a private key but it was stored on the same environment where the system was running.

4.4.6 Role Based Access Control

This scenario was to test the security of access level to the system. The test was conducted by users with different roles and permissions to test access and modification of data in the system. The Database Administrators created users with specific roles and permissions to access specific objects and actions at the Database. The user nurse could only access the data that they had access to, and this was for all other users such as doctors, Health Information Officers and Finance officers. It was observed that the implementation of RBAC in the developed algorithm ensured secure access to the database for both users and applications. Only users and applications with the specific roles and permissions could access data at the database as compared to AES algorithm that did not have any access level controls.

Table 4.5 shows that the overall performance of the developed cryptographic algorithm with Base64, AES of fixed length key of 512 bits was found to be acceptable in all the scenarios that were tested. The developed algorithm scored 80% on the overall parameters while AES scored 67%. However, both the developed algorithm and AES algorithm have equal encryption and decryption speed and the memory usage. Therefore, in conclusion the developed cryptographic algorithm with base64 512 bits has advanced capabilities to ensure enhancement of data protection at the data level. The addition of 512 fixed key length on Base64 algorithm strengthened the security of the developed algorithm

Table 4.5 Performance Test Results and Analysis: Comparison between developed Base64 512 bits algorithm and AES Algorithm.

Algorithm	**Encryption/ Decryption**	**Brute Force attack**	**Known Plain Text Vulnerability**	**Secure Private key Access**	**RBAC**	**Memory usage**	**Overall Score**
Base64 512 bits	0.000017295 3056056518 5547/0.0000 1276421546 930351	Very Strong	Low	Yes	Yes	75.445312 5	80%
AES	0.000062530 9944152832/ 0.000062530 9944152832	Strong	Medium	No	No	75.445312 5	67%

CHAPTER FIVE

DISCUSSION,CONCLUSION AND RECOMMENDATION

5.0 Introduction

This chapter contains three main sections namely, discussion which entails discussion on the key points of the results and the summary of the research findings, conclusion based on the objectives of the research, and the recommendation section which provides the recommendation based on the findings of the research.

5.1 Discussion

5.1.1 Key points of the results and the summary of the research findings of the experiments and simulations

This section describes the key points of the results and the summary of the research findings of the experiments and simulations in a healthcare information system per objective of the study.

Research findings indicated that the developed cryptographic algorithm had a very low risk of known plain text vulnerability, very strong on brute force attack, better on user management with restricted access to the database, fast database performance and a very secure private key. This was attained because of an additional security layer of AES with a fixed key length of 512 bits to Base64 algorithm. Authentication of users and application to the database was implemented as Role Based Access Control and Mandatory Access Control to control user actions and application access at different levels of database access. Comparing cryptographic algorithm Base64 512 bits with the existing algorithms as indicated on *table 4.1* shows that the additional security layer introduced in the developed algorithm of Base64 and fixed length key of 512 bits reduced known plain text vulnerability, improved strength on brute force attack, enhanced ease of data decryption

and performance of the database, improved role-based access control for user management and this made the developed cryptographic algorithm with Base64 512 bits different from other existing cryptographic algorithms.

5.2 Conclusion

This sub section provides a final summary of the research findings with the corresponding research objectives. From the research findings, all the objectives of the study were fully achieved as summarized herein. The following is the summary of the research findings with the corresponding specific objectives of this study.

i. The main objective of this study was to design an enhanced cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems. A cryptographic algorithm with Base64 512 bits model was designed as illustrated in *figure 3.3*, a prototype was developed and tested through experiments and simulations in a healthcare information system. Additional security layer of encryption using Base64 algorithm and use of AES with a fixed key length of 512 bits improved significantly the security of the sensitive data in a healthcare information system.

ii. The second objective of the study was to investigate the existing data encryption algorithms in Healthcare Information Systems and their security characteristics for data protection at the data level. From research findings Symmetrical and Asymmetrical Data encryption algorithms were examined and the following major security characteristics were evaluated and incorporated in the design of cryptographic algorithm with Base 64 512 bits:

    1.Role Based Access Controls

    2. Strength on brute force attack

    3. Known plain text vulnerability

4. Use of private key

5.Ease of encryption and decryption (Database Performance)

Use of security models MAC, RBAC and DAC in the design of the cryptographic algorithm improved on the access controls for users and applications into the database. Use of private key with AES with a fixed key length of 512 bits strengthened the security key for encryption and decryption of the data at the data level in healthcare information systems that store very sensitive data for the patients. Addition of an encryption layer using Base64 algorithm at the database level strengthened brute force attack and reduced the risk of known plain text vulnerability significantly thus a further decrease in data breach in a healthcare information system. Automated database re-indexing for all tables, rows, columns and views improved database performance for encryption (saving of data) and decryption (data retrieval) of data. Healthcare information system was found to perform at optimal speed which reduced fatalities, medical legal cases and improved patient care.

iii. The third objective of this study was to evaluate data protection techniques in Healthcare Information Systems at the data level for integration in the design of the cryptographic algorithm with Base64 512 bits. During the design phase of the cryptographic algorithm with Base64 512 bits the following data protection techniques in healthcare information system were examined and incorporated in the cryptographic algorithm model. Authentication based security techniques that ensured authentication of users and applications into the database, Trust based security techniques that improved on the management of system trust issues, Access control-based security (DAC, MAC, RBAC) that enhanced access control levels for users and applications into the database and Cryptographic based security Models that facilitated in strengthening the encryption and decryption of data.

iv. The fourth objective of the study was to evaluate the performance of the cryptographic algorithm with Base64 512 bits in protecting data in healthcare systems. When the algorithm was fully developed, it was tested to evaluate the performance. The evaluation was conducted in both experiments and simulations. Some scenarios were evaluated via experiments such as, role-based access controls, strength on brute attack and database performance which involved encryption and decryption to determine the speed of data retrieval and data saving. Known plain text vulnerabilities and use of private key was simulated in a simulator. Thorough and extensive evaluation of the performance of the developed cryptographic algorithm with Base64 512 bits ensured that the algorithm met the main objective of the study and that the algorithm exceeded most of the preferred major security characteristics of a good cryptographic algorithm as it was identified from literature review.

5.3 Recommendation

This section gives the take home message of what to DO or NOT to DO based on the findings foregoing and the conclusions. From the research findings it shows that patient data is very sensitive and critical and may even cause death if it is delayed. Patient data is very expensive, valuable and a greater target by cyber criminals. Therefore, there is need for continuous improvement and new innovations on data protection techniques and cryptographic algorithms at the data level in healthcare information systems at the same rate or above the rate at which the cyber criminals are inventing new ways of attack daily. As cryptographic algorithms are developed to enhance data protection at the data level by additional of the number of bits in the algorithm, the performance of the database may slow down and therefore causing delays. The developed cryptographic algorithm with Base64 512 bits would improve data protection of any sensitive and critical data at the data level but especially hospitals, government institutions that store personal sensitive information

of its citizens, Military and examination bodies of any country. For future Research Work, since this study was based on literature review a further research could be conducted in real life systems to compare the effectiveness of the major security characteristics: Known plain text Vulnerability, Strength on brute force attack, use of RBAC, use of private key, ease of decryption and database performance. For optimal testing and better results on the performance of the algorithm all the preferred major security characteristics can be conducted both on experiment and simulation in several health care facilities. Due to limitations on time only few health care facilities participated in the pilot study. The sources of data for analysis in this study was secondary, for further research, primary sources of data for analysis such as interviews and questionnaires can be used to obtain data for analysis in the study.

REFERENCES

Ahmed A, A. Y. (2018). Enhanced tiny encryption algorithm for secure health authetication system. *International Journal of Information Privacy, Security and integrity* .

Babatunde A, T. A. (n.d.). Information Security in Health Care centre uing cryptography and steganonography. *Information Security in Health Care centre uing cryptography and steganonography*.

Devin Partida, Editor-in-Chief, ReHack.com. (2022, February). *5 Biggest Challenges of Health Care Data Security in 2022*. Retrieved from https://www.healthitanswers.net/5-biggest-challenges-of-health-care-data-security-in-2022/.

Diamantopoulou V, A. K. (n.d.). Privacy data Management and awarenes is for public administrations: A case study from the health care domain. *Lecture notes in Computer Science(Including sub series Lecture notes in Artificial Intelligence)*.

George J, B. T. (2019). Security,Confidentiality and privacy in Health of Healthcare Data. *International Journal of trend in Scientific Research and Develpment (2019) Volume 3*.

Harman L, F. C. (2012). State of the art and science Electronic Health Records: Privacy,Confidentiality and security. *State of the art and science Electronic Health Records: Privacy,Confidentiality and security*.

J, P. (2020). An Enhanced Cryptographic Algorithm in Securing Healthcare Medical Records. *Proceeding-2020 3rd International Conference and Vocational Education and Electrical* .

Lucca A, S. L. (2020). A case study on the devlopment of a data privacy management solution based on patient information . *Sensors(Switzerland).*

Medical, s.-c. (2023). https://www.scott-clark.com/. *scott-clark Medical* , https://www.scott-clark.com/blog/types-of-information-systems-used-in-healthcare-facilities/#:~:text=A%20health%20information%20system%20(HIS,send%20patients'%20electronic%20medical%20records.

P, R. W. (2004). *A Multi-Purpose Implementation of Mandatory Access Control in Relational Database Management Systems.*

Press, N. A. (1994). Health Data in the Information Age . *National Academies Press(1994).*

R, P. J. (2019). Hill cipher modification: A simplified approach. *2019 IEEE 11th International Conference on Communication Software and Networks, ICCSN 2019.*

Sanas R, S. M. (2020). Secure Medical Records System using Cryptography . *Secure Medical Records System using Cryptography* .

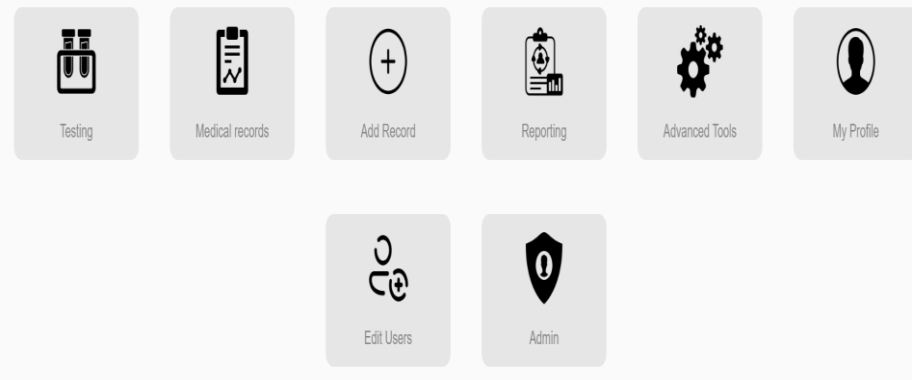
Sari C, R. E. (2018). Cryptography Triple Data Encryption Standard(3DES) for Digital image Security. *Scientific Journal of Informatics(2018).*

W, A.-H. (2010). Cryptography based access controlling healthcare Web systems. Proceedings of the 2010 Information Security Curriculum Development Annual Conference.

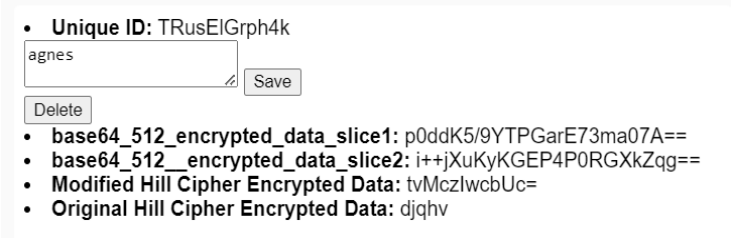
APPENDICES

Appendix I: Cryptographic Algorithm with Base64 512 Bits Source Code

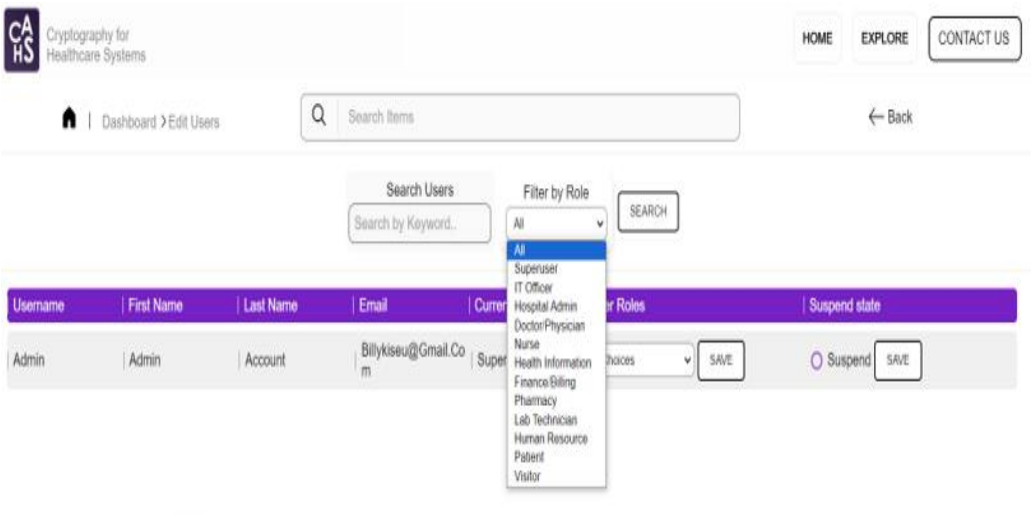
Home Screen Page



Data Encryption and decryption



Role Based Access Controls


Cryptography for Healthcare Systems
HOME
EXPLORE
CONTACT US
Dashboard > Edit Users
Search Items
Back
Search Users
Search by Keyword..
Filter by Role
All
SEARCH
All
Superuser
IT Officer
Hospital Admin
Doctor/Physician
Nurse
Health Information
Finance/Billing
Pharmacy
Lab Technician
Human Resource
Patient
Visitor
Username
First Name
Last Name
Email
Roles
Suspend state
Admin
Admin
Account
Billykiseu@Gmail.Com
SAVE
Suspend
SAVE

APPENDIX II: Cryptographic Algorithm With Base 64512bits Observation Guide

Participants

Cryptographic Algorithm with Base64 512 bits Observation Guide

Participants:

Senior Database Administrators, System Administrators and Senior Security Officers

Test Code	Scenario	Description	Remarks	Signature
001	Encryption and Decryption Process	To test the viability of the algorithm. **Steps:** Input of data into the system, varied types of data using CRUD (create, read, update, delete functionality) and verifying the raw data in the database to be encrypted as these operations are done.	The developed Algorithm meets the criteria for characteristics of cryptographic algorithm as required.	Senior Security Officer JACOB SHERETA

002	Turn Around Time for encryption and decryption	To test the amount of time taken to encrypt and decrypt data during storage and retrieval processes. **Steps:** Measuring the time delay on encrypted and decrypted data CRUD operations compared to unencrypted fields.	Cryptographic Algorithm with Base64 512 bits performed at optimal speed for both storage and retrieval process	System Admin Billy Kisey
003	Size of the data	To test time taken to decrypt and encrypt different sizes of data. **Steps:** Two types of test data. One significantly bigger than the other, then testing the time delay between the CRUD operations of the two	The speed of the developed algorithm was not degraded despite changes in the data size	System Admin Billy Kisey

		sets of data		
004	Strength on Brute force attack	To test the strength of the Algorithm for brute force attack. **Steps:** Attempt to gain access to the system through systematic guessing of password at login for example.	The developed algorithm was very strong on brute force attack. Thus, guess password could not penetrate the database, because a robust password policy has been implemented	Senior Security Officer JACOB SHERETA
005	Known Plain text Vulnerability	To test the level of vulnerability for known plain text. **Steps**: using encrypted plain text and altering it as is, to see the change when the data is decrypted. Examining the Master logs for the record of changes.	The developed algorithm had a very low vulnerability on known plain text. A very small change on plain text resulted into a very huge change on the cipher text. A notification was immediately sent to DBAs and System Security officers for immediate action. Audit logs were also created to keep a record of the change	Senior Security Officer JACOB SHERETA

006	Use of Private Key	To test the importance of the private key in the Algorithm and secure storage of the private Key **Steps:** Examining the storage location and method for the Private Key.	The private Key on the developed algorithm enhanced the security of data access at the database level. The private Key was stored securely and accessible to authorized users only	DB Admin Maghanga Festus
007	Role Based Access Control	To test the security of access level **Steps:** Using accounts with different to test access to and modification of data in the system.	The implementation of RBAC in the developed algorithm ensured secure access to the database for both users and applications	DB Admin Maghanga Festus