Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2024, *7*(1), 11-22.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0701.02011m

Data Protection in Healthcare Information Systems Using Cryptographic Algorithm with Base64 512 bits

Agnes K. Muthaura & John Kandiri

Kenyatta University, School of Applied Sciences, Nairobi, KENYA

Received: 4 April 2024 ▪ Revised: 3 July 2024 ▪ Accepted: 9 August 2024

Abstract

Recent advancement in technology in Healthcare Information Systems has led to a rise in cyber-attacks and data leakages 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 in the design and development of data protection methods. In this study, science research methodology was used to design and develop a cryptographic algorithm with Base64 512 bits to enhance data protection at the data level. The algorithm was tested in a healthcare information system through experiments and simulations. The performance of the algorithm was tested to evaluate encryption and decryption process, strength on brute force attack and plain text vulnerability. The results of the observations showed that the developed algorithm with Base64, AES with fixed length of 512 bits, achieved optimal performance.

Keywords: mandatory access controls, role based access controls, discretionary access controls, label based access controls, advanced encryption standard, electronic medical records.

1. Introduction

Healthcare Information System is a system that is used in a healthcare facility to capture and store patient's data (Scott-Clark, 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 (Scott-Clark, 2023). 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 (Scott-Clark, 2023). 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 et al., n.d.). 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.). Almost all healthcare organizations have encountered no less than one data breach, costing million dollars on average per organization (Babatunde et al., n.d.). The level of security and data protection in Healthcare Information Systems varies from one healthcare facility to the other. 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

Correspondence: Agnes K. Muthaura, Kenyatta University School of Applied Sciences, Nairobi, KENYA.

vital signs, allergies, diagnosis, investigations, medications, assessment, recommendations and patient medical history (Scott-Clark, 2023). 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 (Devin Partida, 2022). 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. 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) (Diamantopoulou et al., 2017a). Electronic Medical Records in Healthcare Information Systems must be protected using enhanced cryptographic algorithm at the data level. The main objective of this study was to develop an enhanced cryptographic algorithm with Base 64 512 bits to protect data at the data level.

2. Background

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. 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 (Diamantopoulou et al., 2017a) and this calls for improved data protection algorithms in healthcare data using enhanced Cryptographic Algorithms. 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. 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 (George & Bhila, 2019). Healthcare facilities and public health sector invests quality time in the data lifecycle (George & Bhila, 2019)

The General Data Protection Regulation goal is protection of sensitive or confidential data and unforeseen risk of data loss or theft, encryption makes sure that all confidential or sensitive information is protected by an agreeable security level at the destination and at the source (Diamantopoulou et al., 2017b).

3. Literature review

This is the detailed literature review of enhanced cryptographic algorithm Base64 512 bits, 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" (Ahmed et al., 2018). 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) (Harman et al., 2012). 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.

3.1 *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. To enhance the algorithm, matrix manipulation is used and uses Mod 26. 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. 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. The modified Hill Cipher has a higher avalanche effect as compared to the original Hill Cipher. 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.

3.2 *Security models*

There are 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). 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. 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.

3.3 *Database security in Healthcare Information Systems*

Database security is incorporated in every database and has several layers and with the security types such as access control, auditing, authenticating and encryption. 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.

From review of the literature, the research identified a gap in the existing types of cryptographic algorithms in healthcare information systems at the data level. The most default security configuration used as cryptographic algorithms to offer data level protection are inadequate and thus the patient data is vulnerable to cyber-attack. MD5 algorithm is used for user authentication and a TDE (Transparent Data Encryption) algorithm that encrypts sensitive data stored in tables and table spaces. This data is transparently decrypted for authorized users and applications to access the data. Transparent Data Encryption algorithm is adequate for data stored

in a media and the decryption security key stored in a separate module from the database (KeyStore), if the hacker happens to hack the password or gain access to KeyStore the patient data would be compromised. A lot of effort has been noticed in identifying the existing cryptographic algorithms in healthcare information systems, a Modified Hill Cipher cryptographic algorithm was identified as the most adequate for enhancing data privacy and protection for sensitive data. This research project informed that the challenge of securing data access at the database level by cryptographic algorithms can be solved by enhancing the existing cryptographic algorithms. "Modified Hill Cipher cryptographic algorithm where cipher text could not be easily predicted and that it has substantial strength and ability to withstand data breach on information ("Health Data in the Information Age," 1994). Modified Hill Cipher cryptographic algorithm had a higher avalanche effect compared to the original Hill Cipher. This means that the Modified Hill Cipher cryptographic method passes the minimum average avalanche effect (Paragas et al., 2019) The average entropy index obtained by the Modified Hill Cipher cryptographic method was higher than the entropy index obtained by original Hill Cipher, which means that the cipher text is unpredictable in Modified Hill Cipher cryptographic method, compared to the original hill cipher, which has a lower entropy index (Paragas, 2020). This modification of original hill cipher to a modified hill cipher demonstrated a significant improvement in strengthening the security of the cipher. This reduces the capability of a known plain text attack by ensuring security at the data 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.

3.4 *Evaluation criteria of acceptable cryptographic algorithm*

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 cryptographic algorithm Base64 512 bits was designed and developed for adequate data level protection.

4. Materials and methods

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 artefact. 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 artefact and thus accurate results.

4.1 *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) 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 artefact 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.

4.2 *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 artefact was designed and developed from the analysis of the security features and characteristics of the existing cryptographic algorithms obtained from literature review.

4.3 *Requirements analysis and data classification*

Requirements for artefact development were obtained from literature review. The requirements for system development were 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 achieve the minimum requirements was identified and the features that did not meet the criteria were improved to develop a cryptographic algorithm Base64 512 bits at the data level. Modified Hill Cipher was identified and the following features were enhanced RBAC, use of private key and ease of data decryption and database performance.

The features and characteristics of existing cryptographic algorithms that were incorporated for artefact development were as obtained from the literature: 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 artefact development were classified accordingly.

4.4 *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.

4.5 *Development phase*

Development of the artefact was done using Python programming language and involved integration of the following data level security measures as identified from literature review: 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. To ensure authentication of users, roles and password profiles 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. To enhance the strength on brute force attack MD5 hashing function encryption algorithm was used to mask passwords permanently and a password policy. 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.

5. Results and analysis

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.

5.1 *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 each specified cryptographic algorithm at the data level. This determined how the cryptographic algorithm Base64 512 bits was designed and developed for adequate data level protection. The evaluation criteria of an acceptable cryptographic algorithm in healthcare information systems were conducted from the literature review and modified hill cipher cryptographic algorithm was identified to have minimum acceptable characteristics for data protection- at the data level. The cryptographic algorithm characteristics for data protection at the data level identified in modified hill cipher were enhanced to develop cryptographic algorithm with Base64 512 bits. The comparison of characteristics for data protection at the data level between modified hill cipher and the developed cryptographic algorithm with Base64 512 bits was conducted by simulation and experiments in a healthcare Information system. Most security characteristics for data protection at the data level of modified hill cipher resulted to perform better than the other algorithms and thus it was considered for comparison with the developed cryptographic algorithm with Base64 512 bits. The results showed that modified hill cipher cryptographic algorithm lacked utilization of RBAC matrix while the developed cryptographic algorithm with Base64 512 bits had RBAC implemented. Modified hill cipher algorithm was weak

on brute force attack and high known plain text vulnerability while cryptographic algorithm with Base64 512 bits was strong on brute force attack and low known plain text vulnerability. Modified hill cipher was slow in encryption and decryption of data for storage and retrieval from the database while the developed algorithm performed at optimum database speed. Both modified hill cipher and the developed algorithm had private key implemented for secure of data access to the database.

5.2 *Data protection techniques Analysis in Healthcare Information Systems at the data level*

The second objective 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. The following are the major data protection techniques as they were obtained from literature review: Authentication Based security, Trust based security, cryptographic based models. Analysis for the identified data protection techniques was conducted to prove that they were the major data protection techniques. 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 as compared to modified hill cipher that had no authentication methods. 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. The results showed that the developed cryptographic with Base64 512 bits enforced trust-based security. From the analysis of the results, it was observed that incorporating trust-based methods in a healthcare information system enhances security at the data level. 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 developed cryptographic algorithm was found to only allow specific users and applications to access and perform specific actions at the database level. The results of the analysis indicated that a secure system is as good as the roles and permissions assigned to users and application to access specific actions at the data level. 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 developed cryptographic algorithm with Base64 512 bits showed that the encryption and decryption of data during storage and retrieval process did not affect database performance as re-indexing of tables, columns, rows and views was configured for automatic database optimization. The results of the analysis indicated that encryption of data at the data level is very critical as health information system stores very confidential data and that speed of database performance is very critical for retrieval and storage of data. During cryptographic based security model's analysis, known plain text vulnerability was tested to find out the impact and effect of a small change in cipher text. This showed that the plain text could not easily be guessed from cipher text. Cryptographic algorithm Base64 512 bits system was designed to incorporate the major database security models in healthcare information systems.

5.3 *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 following are the steps and stages of development of the cryptographic algorithm with Base64 512 bits that were followed to achieve the results of this objective:

1) Model development;
2) functional and non-functional requirements;
3) System design and modelling;
4) experiments and simulations.

5.4 *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 modified Hill cipher for evaluation and validation. The results of the comparison were the empirical evidence which showed that the developed algorithm performed better in terms of data encryption and decryption. The developed cryptographic algorithm with Base64 512 obtained optimal database performance as compared to modified hill cipher. To test the performance of the developed algorithm, various test scenarios were tested by a Senior Database Administrator, Senior Security Officer and Systems Administrator. The analysis of the various scenarios on performance of the cryptographic algorithm with Base64 512 bits were as follows:

5.4.1 *Encryption and decryption process*

The senior security officer 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 Modified Hill cipher which was observed to implement a very weak encryption and decryption technique that follows a known sequence of A to Z substituted into integers 0-26.

5.4.2 *Turnaround time for encryption and decryption*

In this scenario the system administrator 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 modified Hill Cipher that was observed to slow database performance as the size of the data increased.

5.4.3 *Strength on brute force attack*

The senior security officer 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 officer 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 officer 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 as compared to Modified hill cipher which was observed to be weak on brute force attack as the password policy was not implemented.

5.4.4 *Known plain text vulnerability*

This scenario was conducted by a senior security officer 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 modified Hill cipher 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.

5.4.5 *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 modified Hill cipher was observed to obtain a private key but it was stored on the same environment where the system was running.

5.4.6 *Role Based Access Control (RBAC)*

This scenario was to test the security of access level to the system. The test was conducted 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 modified Hill cipher that did not have any access level implemented at all. 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.

6. Discussion and conclusion

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.

6.1 *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 Base64 and of AES with a fixed key length of 512 bits. 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. This enhanced data protection at the data level. Comparing developed cryptographic algorithm Base64 512 bits with the existing algorithms such as modified hill cipher showed that the additional security layer introduced in the developed algorithm of Base64, AES algorithm 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.

6.2 *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.

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, 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. 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: 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. 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.

6.3 *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 and 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 further research could be conducted in real life systems to compare the effectiveness of the major security characteristics. 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 and can be preferably performed by qualified Database Administrators and Systems Security Administrators.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Ahmed, A., Abdulsalam, Y. S., & Olaniyi, O. M. (2018). Enhanced tiny encryption algorithm for secure electronic health authentication system. *International Journal of Information Privacy, Security and Integrity*, *3*(3), 230. https://doi.org/10.1504/ijipsi.2018.10013222

Babatunde, A. O., Taiwo, A. J., & Dada, E. G. (n.d.). *Information security in health care centre using cryptography and steganography*.

Diamantopoulou, V., Angelopoulos, K., Flake, J., Praitano, A., Ruiz, J. F., Jürjens, J., Pavlidis, M., Bonutto, D., Sanz, A. C., Mouratidis, H., Robles, J. G., & Tozzi, A. E. (2017a). Privacy data management and awareness for public administrations: A case study from the healthcare domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10518 LNCS*, 192-209. https://doi.org/10.1007/978-3-319-67280-9_11

Diamantopoulou, V., Angelopoulos, K., Flake, J., Praitano, A., Ruiz, J. F., Jürjens, J., Pavlidis, M., Bonutto, D., Sanz, A. C., Mouratidis, H., Robles, J. G., & Tozzi, A. E. (2017b). Privacy data management and awareness for public administrations: A case study from the healthcare domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10518 LNCS*, 192-209. https://doi.org/10.1007/978-3-319-67280-9_11

George, J., & Bhila, T. (2019). Security, confidentiality and privacy in health of healthcare data. *International Journal of Trend in Scientific Research and Development*, *3*(4), 373-377. https://doi.org/10.31142/ijtsrd23780

Harman, L. B., Flite, C. A., & Bond, K. (2012). State of the art and science electronic health records: Privacy, confidentiality, and security. *American Medical Association Journal of Ethics* (Vol. 14). www.virtualmentor.org712.

Health Data in the Information Age (1994). In *Health Data in the Information Age*. National Academies Press. https://doi.org/10.17226/2312

Lucca, A. V., Silva, L. A., Luchtenberg, R., Garcez, L., Mao, X., Ovejero, R. G., Pires, I. M., Barbosa, J. L. V., & Leithardt, V. R. Q. (2020). A case study on the development of a data privacy management solution based on patient information. *Sensors (Switzerland)*, *20*(21), 1-24. https://doi.org/10.3390/s20216030

Paragas, J. R. (2020, October 3). An enhanced cryptographic algorithm in securing healthcare medical records. *Proceeding – 2020 3rd International Conference on Vocational Education and Electrical Engineering: Strengthening the Framework of Society 5.0 through Innovations in Education, Electrical, Engineering and Informatics Engineering, ICVEE 2020*. https://doi.org/10.1109/ICVEE50212.2020.9243228

Paragas, J. R., Sison, A. M., & Medina, R. P. (2019). Hill Cipher modification: A simplified approach. *2019 IEEE 11th International Conference on Communication Software and Networks, ICCSN 2019* (pp. 821-825). https://doi.org/10.1109/ICCSN.2019.8905360

Rjaibi, W., & Bird, P. (2004). *A multi-purpose implementation of mandatory access control in relational database management systems*. In *Very Large Data Bases*. https://doi.org/10.1016/B978-012088469-8.50088-7