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

Agnes K. Muthaura[1] & John Kandiri[2]

[1]Department of Computing and Information Science, Kenyatta University, Kenya(agnesmuthaura24@gmail.com)

[2]Department of Computing and Information Science, Kenyatta University, Kenya (jkandiri@gmail.com)

https://doi.org/10.62049/jkncu.v4i2.105

Abstract

Due to the recent advancement in technology in Healthcare Information Systems, data leakages at the data level have been on the rise. Therefore, there is need to analyze the existing data protection techniques using cryptographic algorithms in healthcare systems 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 and database security approaches such as enhanced cryptographic algorithms in the design and development of data protection techniques. In this study, design science research methodology was used to design and develop a cryptographic algorithm with Base64 512 bits to enhance data protection at the data level. Python programming language was used to develop a simulation program for experiment. The performance of the developed algorithm was tested in a healthcare information system. The results were compared with the existing cryptographic algorithms to evaluate encryption and decryption process, strength on brute force attack and plain text vulnerability. The results showed that the developed algorithm with Base64 and fixed length of 512 bits achieved optimal performance. In conclusion, healthcare data is very sensitive and critical thus enhanced cryptographic algorithms are necessary to reduce data leakages at the data level.

Keywords: Algorithm, Cryptographic, Security, Encryption, Decryption Standards, Healthcare, Cybersecurity, Healthcare

Introduction

Healthcare Information System is a system that is used in a healthcare facility to capture and store patient's data. 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. 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. 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. Criminal assaults in social insurance have exponentially increased since 2010 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 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 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., 2017) 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 improve data protection at the data level in healthcare systems.

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. 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. 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(*Data_protection_act_2019_kenya*, n.d.)

Literature Review

This chapter describes the detailed literature review of modern cryptographic algorithms. It also reviews 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, improving data protection in Healthcare Information systems is a mandatory requirement and a sensitive activity that requires protection of both subject (users) and objects (data)

There exist various modern cryptographic algorithms for data protection at the data level in healthcare systems. This study reviewed the following modern cryptographic algorithms, Advanced Encryption Standard (AES), Triple Data Encryption Standard (TDES), Data Encryption Standard (DES) and Twofish. The review of the modern cryptographic algorithms combined both asymmetric and symmetric algorithms for data protection at the data level. Many researchers have conducted studies on the performance analysis of these cryptographic algorithms. 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 frontend to backend and improvement on patients care and user experience.

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. 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. 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.

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.

Twofish

Twofish 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. 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. 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.

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.

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., 2020)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.

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 identified cryptographic algorithm at the data level.

Table 1: Evaluation Criteria for 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

The literature informed that a good cryptographic algorithm for data protection at the data level must have a minimum score for each parameter in the following security features and characteristics. This determined how the cryptographic algorithm Base64 512 bits was designed and developed for adequate data level protection.

- Strength on brute force attack,
- Known plain text vulnerability,
- Use of private Key,
- Ease of data decryption
- Database performance,
- Role Based Access Controls

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.

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 analysed 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.

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.

Requirements Analysis and Data Classification

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. From analysis, AES qualified as the most preferred cryptographic algorithm for data protection at the data level. It was therefore identified for enhancement as RBAC and database performance parameters did not meet the criteria. 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
- 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 as shown below:

Table 2: 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

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.

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 of development. 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, AES 512 key length bits was added unto the tradition 256 key length bit. MD5 cryptographic function for encryption was used to mask passwords permanently and a password policy incorporated. 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. Additional of traditional AES bits from standard 256 bits to 512 bits and incorporating with Base64 algorithm at the data level made it very difficult for any malicious attacker whatsoever to guess the plain text from cipher text. To improve on the performance of the database, the database tables, rows, columns and views were optimized for optimal performance.

Results and Analysis

The developed algorithm with Base64 512 bits was evaluated and the empirical evidence results were as shown below.

Table 3: Results and Analysis

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

The developed algorithm with Base64 512 bits scored an average score of 80% for all the security parameters. The security parameters in comparison with the existing cryptographic algorithms were as follows:

- Strength on brute force attack
- Known plain text vulnerability
- Use of private Key
- Ease of data decryption
- Database performance
- Role Based Access Controls

From experimental and simulation results it was observed that the developed cryptographic algorithm with Base64 512 was very strong on brute force attach and very low on known plain text vulnerability. The developed algorithm incorporated use of Private Key and RBAC matrix to allow access to specific authorized users and applications. However, there were no major significant on the memory usage. All algorithms had CPU memory utilization of 75.4453125. From the results it was indicated that the developed algorithm was fast in encryption and decryption of data at a speed of 0.0001729530560565185547 and 0.0001276421546930351 respectively as compared to the existing algorithms thus improved database performance.

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.

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. 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 from an additional security layer of AES with a fixed key length of 512 bits unlike the traditional 256 bits. Authentication of users and application to the database was implemented in a Role Based Access Control and Mandatory Access Control matrix to control user actions and application access at different levels of database access. This enhanced data protection at the data level. Comparing the developed cryptographic algorithm Base64 512 bits with the existing algorithms 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 encryption and decryption, improved performance of the database, improved role-based access control for user management. The enhancement of the existing cryptographic algorithms improved significantly the data protection at the data level in healthcare systems.

Conclusion

This sub section provides a final summary of the research findings. From the research findings, all the the identified security parameters scored an average score of 80% for the developed algorithm as compared to the existing algorithms which scored as follows: Twofish 67%, AES 50%, TDES 42% and DES 22%. For data protection to be enhanced at the data level in healthcare systems, brute force attack, known plain text vulnerability, use of private Key, RBAC matrix and database performance are key security components that must be incorporated in the design and development of cryptographic algorithms. 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 and the results compared with the performance of the existing cryptographic algorithms.

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 showed 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. This should be 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.

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.data_protection_act_2019_kenya*. (n.d.).

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. (2017). 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

Ed Oswald. (2022, December 16). *What Is the Advanced Encryption Standard (AES)?* https://www.usnews.com/360-reviews/privacy/what-is-advanced-encryption.

Ferraris, D., Fernandez-Gago, C., Roman, R., & Lopez, J. (2023). A survey on IoT trust model frameworks. *Journal of Supercomputing*. https://doi.org/10.1007/s11227-023-05765-4

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

Lee, S. B., Kim, Y. H., Kim, J. W., & Song, C. Y. (2020). A design of MAC model based on the separation of duties and data coloring: DSDC-MAC. *Journal of Computer Science*, *16*(1), 72–91. https://doi.org/10.3844/jcssp.2020.72.91

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

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. In *International Journal of Web Information Systems*, 18, (2–3, pp. 156–180). Emerald Publishing. https://doi.org/10.1108/IJWIS-04-2022-0077

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

Rahul Awati. (2021, December). *What is the Twofish encryption algorithm?* https://www.Techtarget.Com/Searchsecurity/Definition/Twofish.

Retracted: Application Research of Data Encryption Technology in Computer Network Information Security. (2023). *Security and Communication Networks*, *2023*, 1–1. https://doi.org/10.1155/2023/9873584

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

Vijayaraghavan#1, N., Narasimhan#2, S., & Baskar#3, M. (2018). A Study on the Analysis of Hill's Cipher in Cryptography. *International Journal of Mathematics Trends and Technology*, *54*(7). http://www.ijmttjournal.org