International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

System and Method to Provide a Keyless Mechanism to Encrypt/Decrypt Memory Context

Amit Rai[1], Puja Kumari[2], Naveen Rai[3]

[1]Technical Lead, Thales
[2]Software Developer, Kogo
[3]Technical Lead, Telus

Abstract
In contemporary computing environments, safeguarding sensitive data is of paramount importance. Traditional encryption methods often rely on keys, which themselves pose security risks due to potential loss or compromise. In response to this challenge, this paper proposes a keyless mechanism for encrypting and decrypting memory context, leveraging the innovative keyless user defined optimal security (KUDOS) algorithm. Traditional encryption methods rely on cryptographic keys, which pose inherent security risks and complexity in key management. In contrast, the KUDOS algorithm offers a novel approach to encryption without the need for explicit cryptographic keys, providing enhanced security and simplicity in the encryption process. By deriving encryption parameters from the memory context itself, the KUDOS algorithm ensures robust protection of sensitive data stored in memory while eliminating the vulnerabilities associated with key storage and transmission. This paper presents the theoretical foundations of the KUDOS algorithm, along with practical implementation strategies for integrating keyless encryption and decryption mechanisms into memory management systems. Through experimental evaluation and analysis, we demonstrate the effectiveness and efficiency of the proposed keyless mechanism for securing memory context in various computing environments. The KUDOS algorithm holds significant promise for enhancing security and privacy in memory management systems, offering a keyless encryption solution that is both robust and scalable.

Keywords: Encryption, decryption, memory, KUDOS

1. Introduction

Cryptography is the application of techniques for encrypting data between the sender and receiver so that the receiver can read the data and an adversary cannot. Making sensitive data safe is critical with the overwhelming dependence on electronic communication systems in the modern world. Data may be transferred without the danger of being intercepted by employing several cryptographic procedures [1-4]. Encryption is the most common way to protect large amounts of text data [5]. Cryptography is a process to convert plain text into cipher using two types of keys; symmetric and asymmetric key. Symmetric means that the same key is used between sender and receiver in encryption and decryption processes. The examples of symmetric keys are substitution, transposition, hill cipher, Play fair cipher, Vigener, and others. While asymmetric key means that there are two keys in encryption and decryption

processing—a private and public key [6-8]. Figure 1 and Figure 2 illustrate the block diagram of the cryptography asymmetric and symmetric keys, respectively. Many approaches, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA), Triple Data Encryption Standard (3-DES) and other established procedures, are used to encrypt and decrypt data [9-11]. However, these approaches are still ineffective at encrypting large-scale text with high redundancy and large storage capacities. To alleviate these issues, researchers have developed various text-to-image encryption algorithms to increase text security and efficiency, thus improving robust cryptographic algorithms.

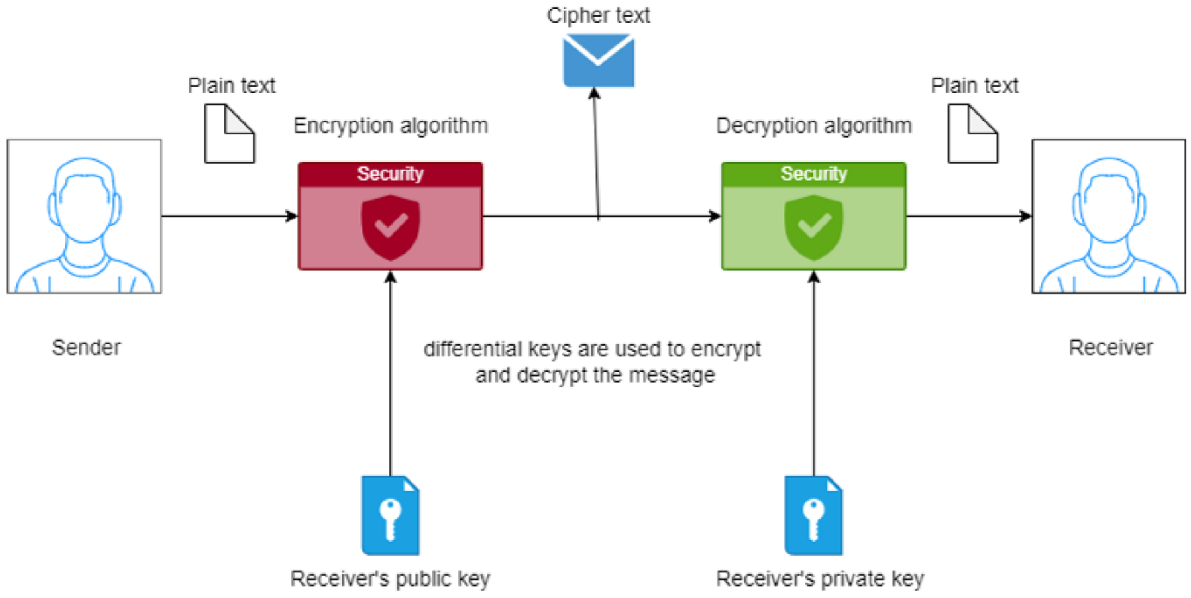

Figure 1: Asymmetric key Cryptography [12]

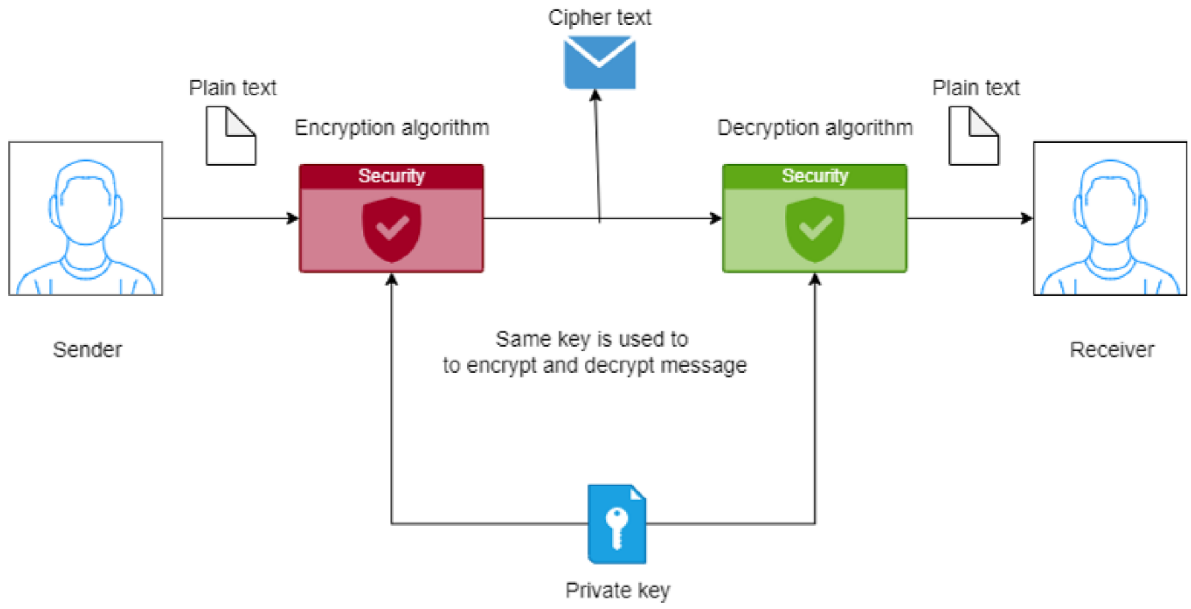

Figure 2: Symmetric Key Cryptography

Classical cryptography uses keys for encryption and decryption. Key generation, key exchange, and key storage are complex problems. Hackers try to exploit the key to attack a system. Attacks based on

differential power analysis can extract cryptographic keys during the encryption and decryption process. Quantum adversaries are targeting key extractions as well [13]. Internet of things (IoT) devices are being used more and more in everyday life. It has become an inevitable part of human life, which can also threaten one's privacy since it might contain information in the communication that a third party should not be aware of. Hence, securing IoT devices is critical [14]. Another drawback of using keys for cryptography, however, is the large memory space allocated for key storage in devices. Most of the IoT devices do not possess ample memory space due to cost constraints and limited power supply [15-17]. This means that the problem of longer secret keys and strong cryptography systems can be hard to implement in IoT devices. These obstacles were a motivation to develop a keyless cryptography scheme [18].

Encryption technology is a secure transmission method. This technology encrypts the data to be transmitted, converting it into cypher text that an authorized person can successfully restore. Several encryption schemes can be used to secure images [19] Figure 1 Encryption algorithms are classified as direct or partial encryption to provide integrity and privacy [20]. All media data is encrypted in full encryption [21]. It can encrypt large amounts of data, making it less efficient but more secure. Only a portion of the media content is encrypted during selective (partial) encryption. Because encryption operations are performed on a small amount of data, partial encryption algorithms reduce encryption and decryption time, making them more efficient but less secure [22][23]. Some researchers have created a single scheme that combines encryption and compression. Encryption and compression are implemented simultaneously in such a scheme [24].

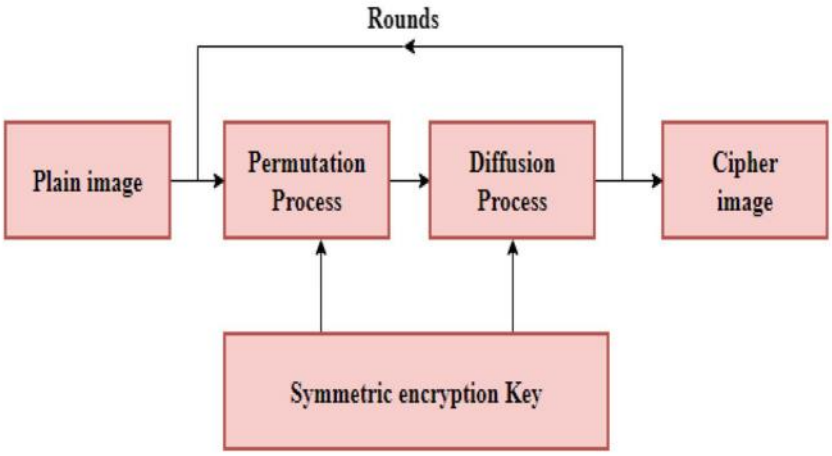

Figure 3: Encryption architecture [25]

2. Review of Literature

Wang et al., (2024)[26] studied in a time marked by the widespread presence of digital technology and the fast growth of large collections of data, it is crucial to prioritize the accuracy and dependability of information. With the rising complexity of cyber threats, classic cryptography approaches are encountering more complicated obstacles. This article aims to investigate the issues related to key exchanges, including their diverse and intricate nature, scalability, and the time metrics connected with different cryptographic operations. We provide an innovative cryptography method that is supported by theoretical frameworks and practical engineering. An essential aspect of this technique is doing a comprehensive investigation of the relationship between Confidentiality and Integrity, which are fundamental principles of information security. Our approach utilizes a staged technique, first with a

thorough analysis of conventional cryptographic procedures, such as Elliptic Curve Diffie-Hellman (ECDH) key exchanges. In addition, we explore encryption and decryption paradigms, ways for generating signatures, and the hashes used for Message Authentication Codes (MACs). Every process undergoes a thorough assessment to determine its level of performance and dependability. A rigorously structured simulation was undertaken to acquire a thorough insight, demonstrating the strengths and areas for future development of different methodologies. Our cryptographic approach earned a confidentiality measure of 9.13 in thorough simulation runs, which is a considerable improvement compared to previous techniques. Moreover, the protocol's robustness is further confirmed by the integrity metrics, which stand at 9.35. The numbers, obtained after rigorous testing, highlight the effectiveness of the protocol in improving data security.

Bahache et al., (2024)[27] examined a biosensor is a device used to detect and communicate several physiological phenomena, such as body temperature, electrocardiogram (ECG), pulse, blood pressure, electroencephalogram (EEG), and respiration rate. This transmission takes place via a Wireless Body Area Network (WBAN) while remotely diagnosing patients using the Internet-of-Medical-Things (IoMT). Nevertheless, while transmitting sensitive data from the Internet of Medical Things (IoMT) over a Wireless Body Area Network (WBAN) using an unsecure channel, it becomes vulnerable to different types of risks. Therefore, it is crucial to establish strong security measures to provide protection against possible adversaries. In order to tackle the security risks related to patient monitoring in healthcare systems and meet the essential criteria for security and privacy in communication, a strong authentication framework is essential. Therefore, it presents a flexible and strong authentication framework for cloud-based healthcare applications, significantly reducing the weaknesses revealed in previous research. This framework is specifically developed to provide protection against quantum assaults by using the Kyber algorithm. The proposed protocol undergoes a formal security verification using AVISPA, as well as an informal verification. Furthermore, a thorough evaluation is conducted to compare the performance and security of the current work with earlier studies. The comparative findings clearly demonstrate that our suggested approach outperforms on both categories.

Rajeshkumar et al., (2024)[28] examined that Big Data (BD) refers to the management, manipulation, and examination of vast quantities of data. The rapid progress in the development of cloud computing in healthcare has made the security and confidentiality of medical information a top priority for healthcare services and apps. Additional cryptographic systems are need to effectively tackle these challenges. This study presents a new Three-Factor Authentication (3FA) and optimum Map-Reduce (MR) architecture for securely transmitting Big Data (BD) via the cloud using Secure Hashing Authentication XOR-ed Elliptical Curve Cryptography (SHAXECC). The authentication process begins by using the SHA-512 algorithm, which safeguards the network from unwanted entry. Subsequently, the process of data deduplication is carried out using the SHA-512 method, which effectively eradicates redundant files. Subsequently, a very efficient MR approach is shown to effectively manage a substantial volume of big data. Within an ideal MR (MapReduce) framework, the mapper employs the Modified Fuzzy C-means (MFCM) clustering technique to first establish the BD (Big Data) clusters. Next, the reducer employs the Levy Flight and Scoring Mutation-based Chimp Optimization Algorithm (LSCOA) to create the ultimate BD clusters. Ultimately, the SHAXECC is used to securely transport the data. Experiments are conducted to assess the superiority of the proposed approach in comparison to current techniques, based on several performance indicators. The suggested technique demonstrated superior performance compared to other existing models in terms of clustering and security measures. The suggested methodology is optimal for ensuring

data security and privacy in cloud-enabled healthcare data.

Rana M. et al., (2023) [29] presents a study on designing and implementing a robust key management scheme for lightweight block ciphers in Internet of Things (IoT) networks. The proposed scheme utilises partial key pre-distribution to achieve lightweight and secure key management. The protocol's security has been analysed against various attacks, demonstrating its resistance. Performance evaluation results indicate that the proposed key management technique is suitable for resource-constraint IoT networks, as it reduces communication overhead, power consumption, and storage space requirements. The results affirm that the proposed solution effectively ensures secure communication in IoT networks. Overall, this research contributes to developing a secure and efficient key management scheme for lightweight block ciphers in IoT networks.

Desoky et al., (2023)[30] Information systems face significant risks from the latest developments in cryptanalysis methods and the unauthorized disclosure of information on the cryptosystem used. An adversary may achieve the decryption of ciphertexts, while users of a certain cryptosystem remain unaware and continue to use the compromised cryptosystem. This study introduces an innovative cryptosystem that utilizes Latin squares and cognitive artificial intelligence/machine learning techniques for blockchain and clandestine communications. This cryptosystem, known as CipherInCipher, has the ability to operate in four different modes: keyless, symmetric, asymmetric, and hybrid encryption. It can encrypt data inside a cipher, making it a versatile and powerful encryption method. CipherInCipher is a unique method that sets itself apart from other approaches, such as obscurity, by being public-based and not relying on the secret of any of its components. It achieves a robust degree of security by using strong ciphertext and effectively prevents adversaries from accessing the real ciphertext, thereby safeguarding sensitive information. The validation research given provides evidence of the strong cryptographic capabilities of CipherInCipher in attaining its intended aim.

Han et al., (2022)[31] analyzed that Hardware security modules (HSMs) have been used as a reliable basis for cloud services. Regrettably, current systems that use HSMs are unable to handle the increasing need for multi-tenant scalability caused by growing trends like microservices, which require frequent cryptographic operations. Cloud suppliers offer Hardware Security Modules (HSMs) as a service, serving as an alternate option. Nevertheless, the use of cloud-managed HSMs in these setups gives rise to security risks because of the untrusted and shared operating environment. Introducing ScaleTrust, an efficient and reliable system designed for the management of cryptographic keys. ScaleTrust enables us to increase the number of virtual HSM partitions, which are individually separated from one another and resistant to assaults from inside the cloud, while maintaining the physical separation of the root of trust. In order to do this, ScaleTrust utilizes Intel SGX and several HSM functionalities, including the ability to limit key use by managing key properties of in-HSM keys and creating a secure channel only via HSM instructions. Ultimately, we implement ScaleTrust on four actual systems: Keyless SSL for TLS private key offloading, JSON Web Token authentication for microservices, key provisioning, and encryption in database systems. Our assessment demonstrates that ScaleTrust effectively accomplishes multi-tenancy via the implementation of numerous virtual HSMs, which use older HSM hardware specifically built to accommodate a single tenant. ScaleTrust offers protection against internal security risks while incurring a throughput and latency cost of 11.9% and 39.0% respectively for Keyless SSL, as opposed to using stand-alone HSMs.

Dua et al., (2022)[32] Ensuring data security is crucial for the transmission of multimedia content. Several cryptographic techniques have been devised to ensure the safe transmission of both textual and visual data.

Due to the substantial bulk of input data and time limitations, there have been limited advancements in the field of video encryption. With the significant rise in digital media transport across networks, ensuring the security of video data has become a crucial aspect of network dependability. Prior to this, block encryption methods and 1D-chaotic maps have been used for the purpose of encrypting videos. While the outcomes achieved via the use of 1D-chaotic maps were quite satisfying, this strategy was hindered by several constraints due to the very limited dynamic behavior shown by these maps. In order to address these limitations, this article suggests a video encryption method that utilizes an Intertwining Logistic Map (ILM)-Cosine transformation. The first stage included dividing the incoming video into several frames, taking into account the frames per second (FPS) number and the duration of the movie. Subsequently, each frame was individually chosen, and the association between the pixels was diminished by the use of a technique known as permutation/scrambling. Furthermore, each frame was subjected to a 90° counterclockwise rotation in order to provide further unpredictability into the encryption process. In addition, the random order replacement method was used to make alterations to each picture, both horizontally and vertically. Ultimately, the encrypted frames were rearranged based on a frame selection key and combined to produce an encrypted video, which was then sent to the user as the final result. The efficacy of this approach was assessed by evaluating the status of several metrics such as Entropy, Unified Average Change in Intensity (UACI), and correlation coefficient (CC). The proposed methodology also performs decryption of the encrypted video, and the quality of the decryption was evaluated using metrics such as mean square error (MSE) and peak signal-to-noise ratio (PSNR).

Noura et al., (2021)[33] In recent times, academics, standardization bodies, communications sectors, and energy suppliers have been actively working towards achieving resilient and efficient communication in Smart Grids. In order to fulfill these criteria, a novel iteration of Narrow-Band Power Line Communication (NB-PLC) protocols has been suggested. One major benefit of PLC systems is their cost-effectiveness, since they do not need any new expenses for deployment and wiring. This is because the existing power lines may be used to transport both power and data concurrently. PLC technology is widely used in Smart Grids for several purposes, including enhanced metering infrastructure, distributed automation, street light management, and public charging. A widely used PLC standard is PRIME (Power-line Related Intelligent Metering Evolution). This technology facilitates many Smart Grid services across energy distribution networks. PRIME employs security measures at the data connection layer to specifically address data confidentiality and message authentication, while excluding data availability. This article presents a highly effective and resilient security solution designed to protect against attacks that compromise availability and secrecy. The primary objective of the proposed method is to improve the security and dependability of PLC communication between end nodes, while minimizing the additional burden on resources, complexity, and latency. The approach relies on the use of the Information Dispersal Algorithm (IDA) in conjunction with the inherent properties of Power Line Communication (PLC) channels. Specifically, the proposed technique allows end nodes to derive cryptographic primitives by using a shared working key and random channel parameters, resulting in benefits for these nodes. The security and performance tests demonstrated that the suggested approach has little impact on system resources while providing a high level of accessibility and enhancing data privacy.

Cambou et al., (2020)[34] examined that the low power networks often lacks sufficient computer power to implement widely used cryptographic techniques. Additionally, many systems need significant computational power, which may make them vulnerable to side channel attacks. This article presents a technique known as "cryptography with analog scheme using memristors," which exploits the physical

characteristics of memristors. Memristors are active elements that are well-suited for designing components like artificial neurons. The suggested devices use encryption by dividing messages into blocks of bits. Each block modulates the injected currents into randomly chosen memristor cells, which then produce sets of resistance values that are transformed into cipher texts. The connecting devices separately create identical addresses using hash-protected handshakes. These addresses simultaneously refer to the same set of cells in the arrays and their pictures. These block ciphers, such as those that are 1 KB in length, can only be decrypted using the same memristor array that is controlled by analog circuitry or its image, rather than relying on digital key-based methods. The suggested approaches produce cipher text and decode it with an energy consumption of around one femtojoule per bit, which falls below the detectable threshold for differential power analysis. The essay elucidates the possibilities of using distinct cells for each message encryption, operating under diverse circumstances, to alleviate conventional assaults. The text offers an in-depth analysis of memristors to assess the practicality of the method and explores various hardware and architectures for implementing the proposed system.

Sengupta et al., (2020)[35] intended that the increasing popularity of the Internet of Things (IoT) in recent years has created a potential prospect for the development of home automation systems and industrial applications. The Industrial Internet of Things (IIoT) is facilitated by using these advantages, leading to the implementation of automation in many sectors. The Internet of Things (IoT) is susceptible to several cyberattacks and requires innovative strategies to attain the appropriate level of security. Furthermore, the advent of IIoT has intensified the potential harm caused by its security flaws. Hence, this study aims to categorize assaults largely by the items that are vulnerable, in order to provide guidance to researchers. Afterwards, each of the specific assaults is correlated with one or more levels of the comprehensive IoT/IIoT framework, followed by an analysis of the responses suggested in existing literature. Within this framework, we thoroughly examine a particular Blockchain architecture called Tangle, which is specifically tailored for the Internet of Things (IoT). We go into its advantages and disadvantages in great depth. We emphasize the most relevant Blockchain-based solutions that have been offered recently to address the issues presented by conventional cloud-centric apps. The essay discusses the blockchain solutions offered in the context of two significant applications for both IoT and IIoT. Afterwards, we create a classification system of the security research fields in IoT/IIoT, including the appropriate remedies for each. Ultimately, this study identifies other open research paths that are pertinent to its main topic.

Zhu Y. et al., (2020) [36] introduces an extended protocol using keyless encryption, which is hash-based and generic in cryptography. The sender side and the receiver side will be contained in the protocol. The sender will encrypt a plaintext and then send the cipher to the receiver side, and the cipher used in the protocol will be based on memristor arrays. We will use values of blocks of the plaintext to sort the cipher, which will improve the difficulty of being deciphered. Then, the receiver will receive the cipher and use it to decrypt the plaintext. The method of implementation is thoroughly detailed in this paper, and the security of the protocol is evaluated by testing random plaintexts thousands of times.

Hu et al., (2019)[37] deploying content delivery networks (CDNs) on cloud platforms has the capacity to enhance performance by strategically positioning resources and caches in proximity to subscribers. Preventing data leakage on an untrusted public cloud is of utmost importance, particularly when it comes to safeguarding sensitive information like the SSL private key. The widely used Keyless SSL solution enables content owners to maintain control of SSL private keys on their own key servers located on their premises. However, this solution is likely to result in performance limitations and hinder the flexibility of

Content Delivery Networks (CDNs). This article presents a new key management system called STYX, designed to securely transport trustworthy data via unreliable networks and store it on untrusted platforms. STYX enables the safe supply of keys for CDN scale-out, ensuring that the key is secured with comprehensive revocation rights for CDN scale-in. The implementation of STYX is a three-phase hierarchical key management method, using Intel Software Guard Extensions (SGX) and QuickAssist Technology (QAT). In addition, STYX facilitates CDN services by including Nginx as the SSL termination proxy and the widely-used Redis/Memcached/Apache as backend caching engines. The performance assessment demonstrates that STYX outperforms the native HTTPS servers on the CDN node owing to QAT acceleration, resulting in a substantial 5-fold increase in throughput and a 50% decrease in latency.

Wang Z. et al., (2019) [38] designed the Dynamically Reconfigurable Encryption and Decryption System, which is based on Field Programmable Gate Array. Considering the functional requirements, the cryptographic algorithm reconfigurable module files stored in External Memory could be configured dynamically into the assigned on-chip Reconfigurable Partition, supported by Core Controller and the Reconfiguration Control Platform. The experiment results show that, compared with the Static Encryption and Decryption System, our design reduces the logic resources by more than 30% and completes the algorithm swapping at the configuration speed of 15,759.51 Bytes/ms. It indicates that our design could reduce logic resources consumption and improve utilization efficiency and system flexibility.

3. Problem statement

In the context of secure data handling and protection, traditional encryption methods often rely on cryptographic keys for encrypting and decrypting sensitive information stored in memory. However, the management and protection of these keys pose significant challenges, including key storage vulnerabilities, key distribution complexity, and potential exposure to attacks. Additionally, key-oriented algorithms are very efficient, but handling them might be complex due to the need of managing keys. During the process of producing encryption keys, a significant amount of energy is used. This energy expenditure is responsible for reducing the overall speed of data transmission and negatively impacting battery life. To address these challenges and enhance the security of data encryption and decryption processes, there is a need for a keyless mechanism that can effectively encrypt and decrypt memory context without the requirement of cryptographic keys. This keyless approach should provide robust protection for sensitive data stored in memory, while also mitigating the risks associated with key management and distribution. The keyless mechanism should leverage innovative cryptographic techniques or algorithms that eliminate the need for explicit keys while ensuring strong encryption and decryption capabilities. Additionally, the solution should be scalable, efficient, and compatible with existing hardware and software systems to facilitate seamless integration and deployment in diverse environments. Overall, the objective of this proposed system and method is to provide a secure, keyless mechanism for encrypting and decrypting memory context, thereby enhancing data security and mitigating the vulnerabilities associated with traditional key-based encryption approaches. By addressing these challenges, the proposed solution aims to enable robust protection of sensitive data in memory and enhance the overall security posture of computing systems and applications.

4. Research Methodology

The majority of cryptographic algorithms may be classified into one of two categories. However, the tec-

hnique presented here employs a hybrid approach, combining both stream and block ciphers. Exclusively sequence counters are used. The sequence counters possess a well-defined initial point and a specific increment value. The sequences are integrated with the current data at a certain level (to be explained later) and the encrypted data subsequently substitutes the original data. The sequence counters in the proposed approach are used at the following levels: Block level refers to the highest level where characters inside a block or line are rearranged based on the sequence counter. Character level - Each character has a corresponding ASCII value that may be combined with the sequence counter. The provided example falls within this category. The binary level, often known as the lowest level, refers to the most fundamental level of computer processing. The computation performed here is only in binary form, using just the digits 0 and 1. Bit level calculations provide enhanced security since their effects are observable at all levels above, including the character level. The proposed approach incorporates both stream cipher and block cipher techniques to augment security by using the benefits of both, namely, high diffusion and bit-level security. Since the KUDOS is determined by the user, the user has the ability to choose the beginning point of the series. Each level is equipped with sequence counters that have varying increment values. The user has the ability to choose a custom starting number for the counter. This information will then be included in a packet and added to the encrypted data. If the user does not provide a starting point for the sequence counter, default values will be used and there will be no need to add anything to the encrypted data. This is the reason why it is referred to as a user-defined algorithm. The technique of the task will need the employment of a keyless user-defined optimum security algorithm, which will be enhanced by including a unique number to ensure security throughout the process of uploading and downloading documents. This algorithm will then carry out the encryption and decryption of the text document. Figure 3 depict the proposed framework which is defined in terms of encryption and decryption process as shown below.

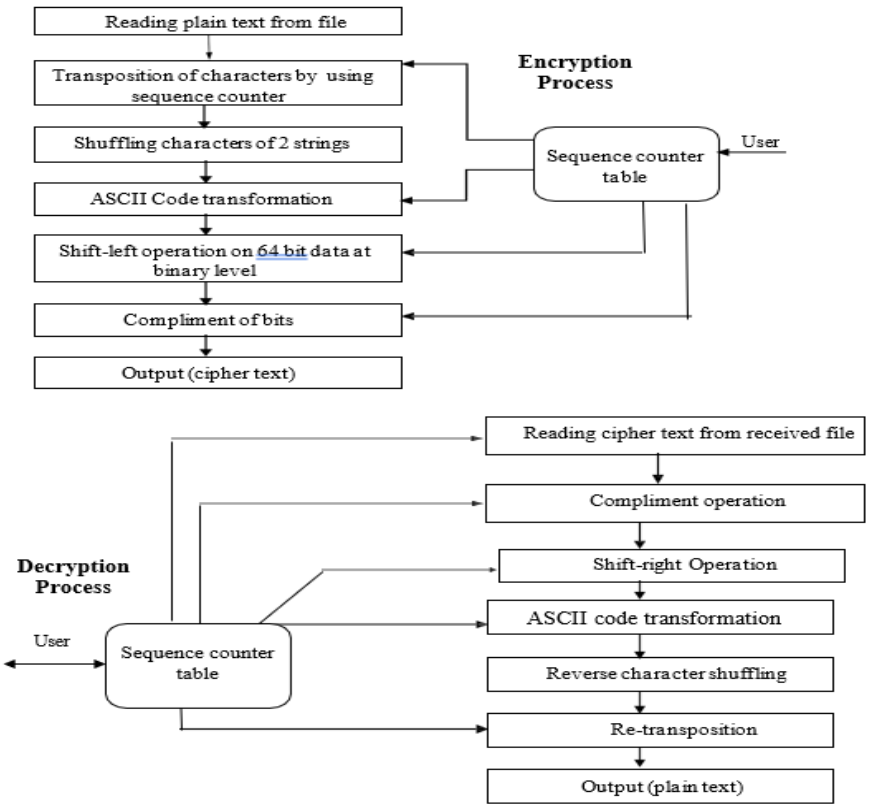

Figure 3. Proposed framework

Encryption process

This algorithm is based on the idea of maintaining a balance between security and speed of an algorithm. In this algorithm, two stacks are taken. First stack holds the information about sequence counter and other stack maintains record for the data on which encryption has to be performed. The encryption process is described below.

At the beginning of the process, it reads plain text from the file line by line and then Character transposition is accomplished by the use of sequence counter, and the user gets to choose the sequence counter that best suits his preferences. Following the completion of the stage, two strings are selected from the file, and both of them are shuffled by sequentially putting one character from the first string and the first character from the second string. This encryption does not rely on particular users. When the third step is performed, the output from the second step is used as input, and the characters are converted into ASCII code. Following that, the shift-left operation is carried out on the 64-bit data at the binary level. Complement is the foundation upon which the encryption process is carried out. Following the completion of the fourth step, the sequence of bits is complemented, and the subsequent sequence of the same number of bits is left unmodified. It is necessary to repeat the whole system until the plaintext is transformed into the encrypted text. Due to the fact that it is dependent on a sequence counter, the system does not own an encryption key. The sequence counter is made up of four bytes, and each byte that makes up the sequence counter represents one encryption step. The combination of four sequence counters results in the formation of an encoding key. It is possible for the user to specify the sequence counter, which will result in the combined key being sent together with the data to be encrypted at the receiving end. In any other case, the encryption process is carried out using the default sequence.

Decryption Process

The decryption procedure is the exact inverse of the encryption process. The appropriate sequence counters are determined from the sequence counter table for the decryption process. The decryption method has been described below:

In the beginning, it is reading encrypted text from the file that was received, and the procedure includes getting the sequence counter from the central database server and carrying out a binary-level complement operation. In the second phase, the changed cipher text is subjected to the shift-right operation, and the ASCII codes are converted into characters. It is necessary to do reverse shuffling in order to get intermediate cipher text, which is then used in the third stage. All of the processes are repeated until the cipher text is turned into plain text, and the last phase involves the re-transposition of characters that are contained inside a single line.

5. Result and discussion

Based on the information provided in table 1 and figure 4, it can be inferred that the suggested method has a shorter execution time compared to the current methods. Time is measured in milliseconds.

Table 1. Time taken of proposed method with other techniques

Algorithm Name	Time (ms)
HRSA	223
MRSA	208
Proposed method	188

Figure 4 depict the comparison of time of proposed method with other existing method as shown below. From this figure, the HRSA method attained maximum time taken while MRSA method obtained minimum time taken, which is slightly lower than to HRSA method. Therefore, it is clear that the proposed method achieved minimum time taken as compared to HRSA and MRSA method as shown below.

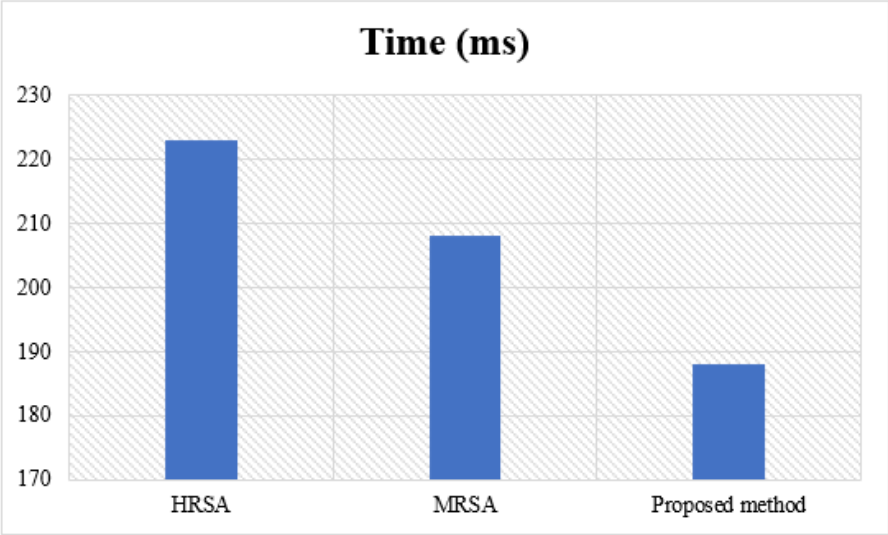

Figure 4. Comparison of Time

Based on the information provided in the table 2 and figure 5, it can be inferred that the suggested method has a shorter encryption and decryption time compared to the current techniques. Time is measured in milliseconds as shown below.

Table 2. Time taken of Encryption and Decryption

Algorithm Name	Encryption Time in ms	Decryption Time in ms
HRSA	1639	3125
MRSA	1583	3521
Proposed Methods	1249	2765

Figure 5 depict the comparison of time taken of encryption and decryption of proposed method with other existing method as shown below. From this figure, the HRSA method attained maximum time taken in encryption and decryption while MRSA method obtained minimum time taken of encryption and decryption, which is slightly lower than to HRSA method. Therefore, it is clear that the proposed method achieved minimum time taken of encryption and decryption as compared to HRSA and MRSA method as shown below.

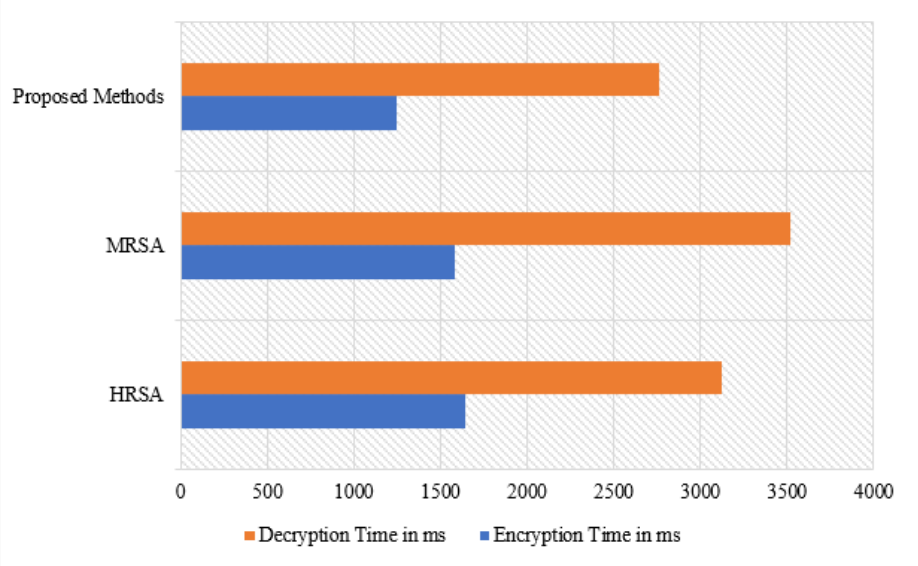

Figure 5. Time taken of encryption and decryption

6. Conclusion and future scope

In conclusion, the system and method proposed provide a robust and efficient solution for implementing a keyless mechanism to encrypt and decrypt memory context. By leveraging innovative techniques and algorithms, the system addresses the critical challenge of securing sensitive data in memory without relying on traditional cryptographic keys. The keyless approach offers several advantages, including enhanced security, reduced vulnerability to key-based attacks, and simplified key management. By eliminating the reliance on cryptographic keys, this approach offers enhanced protection against key exposure, loss, or compromise, thereby mitigating potential security risks associated with traditional encryption methods. From the comparative graphs, it is clear that the proposed method attained low time taken in terms of encryption and decryption as compared to HRSA and MRSA method. In future, we will be exploring opportunities to integrate the keyless mechanism based on the KUDOS algorithm with emerging technologies such as blockchain, homomorphic encryption, and secure multiparty computation to address evolving security challenges and enable novel applications in decentralized and privacy-preserving computing environments.

References

1. Jebur, R.S.; Der, C.S.; Hammood, D.A. A Review and Taxonomy of Image Denoising Techniques. In Proceedings of the 6th International Conference on Interactive Digital Media (ICIDM), Bandung, Indonesia, 14–15 December 2020; pp. 1–6.
2. Singh, A.; Gilhorta, R. Data security using private key encryption system based on arithmetic coding. *Int. J. Netw. Secur. Its Appl.* **2014**, *2*, 58–67.
3. Singh, S.; Jain, A. Combination of RGB Substitution for Text to Image Encryption Technique using AES. *Spvryans Int. J. Eng. Sci. Technol.* **2015**, *2*, 1–7.
4. Naji, M.A.; Hammood, D.A.; Atee, H.A.; Jebur, R.S.; Rahim, H.A.; Ahmad, R.B. Cryptanalysis cipher text using new modeling: Text encryption using elliptic curve cryptography. *AIP Conf. Proc.* **2020**, *2203*, 020003.

5. Abusukhon, A. Block cipher encryption for Text-to-Image Encryption algorithm. Int. J. Comput. Eng. Technol. (IJCET) 2013, 4, 50–59. Available online: https://www.researchgate.net/publication/282656379 (accessed on 6 February 2022).
6. Padhiar, S.; Mori, K.H. A Comparative Study on Symmetric and Asymmetric Key Encryption Techniques. In *Implementing Data Analytics and Architectures for Next Generation Wireless Communications*; IGI Global: Hershey, PA, USA, 2022; pp. 132–144.
7. Kapoor, J.; Thakur, D. Analysis of Symmetric and Asymmetric Key Algorithms. In *ICT Analysis and Applications*; Springer: Singapore, 2022; pp. 133–143.
8. Alaya, B.; Sellami, L. Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks. *J. Inf. Secur. Appl.* **2021**, *58*, 102779.
9. Naji, M.; Hammood, D.A.; Atee, H.A.; Yahia, S. Implantation of Caesar and Hill Cipher on Database for Better Security. *Eur. J. Technol. Eng.* **2019**, *18*, 24.
10. Ibada, A.J.; Ehkan, P.; Ngadiran, R.; Hammood, D.A.; Alkhayyat, A. RGB Image Encryption using Hill Algorithm and Chaos System. *J. Physics: Conf. Ser.* **2021**, *1962*, 012061.
11. Patil, P.; Narayankar, P.; Narayan, D.G.; Meena, S.M. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Comput. Sci.* **2016**, *78*, 617–624.
12. Noor, Noor Sattar, Dalal Abdulmohsin Hammood, Ali Al-Naji, and Javaan Chahl. "A fast text-to-image encryption-decryption algorithm for secure network communication." *Computers* 11, no. 3 (2022): 39.
13. . B. Cambou, M. Gowanlock, B. Yildiz, D. Ghanaimiandoab, K. Lee, S. Nelson, C. Philabaum, A. Stenberg, and J. Wright, "Post quantum cryptographic keys generated with physical unclonable functions," Applied Sciences, vol. 11, no. 6, p. 2801, 2021.
14. M. Keshavarz and M. Anwar, "Towards improving privacy control for smart homes: A privacy decision framework," in 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1–3, IEEE, 2018.
15. B. Cambou, D. H´ely, and S. Assiri, "Cryptography with analog scheme using memristors," ACM Journal on Emerging Technologies in Computing Systems (JETC), vol. 16, no. 4, pp. 1–30, 2020.
16. R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, no. 9, pp. 51–58, 2011.
17. N. Baracaldo, L. A. D. Bathen, R. O. Ozugha, R. Engel, S. Tata, and H. Ludwig, "Securing data provenance in internet of things (iot) systems," in International conference on service-oriented computing, pp. 92–98, Springer, 2016.
18. Miandoab, Dina Ghanai, Sareh Assiri, Joseph Mihaljevic, and Bertrand Cambou. "Statistical analysis of ReRAM-PUF based keyless encryption protocol against frequency analysis attack." *arXiv preprint arXiv:2109.11075* (2021).
19. David VARS, Govinda E, Ganapriya K, Dhanapal R, Manikandan A (2023) An automatic brain tumors detection and classifcation using deep convolutional neural network with VGG-19," 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). Coimbatore, India. pp. 1–5.
20. Lian S, Liu Z, Ren Z, Wang H (2006) Secure advanced video coding based on selective encryption algorithms. IEEE Trans Consum Electron 52(2):621–629.
21. Xue X, Palanisamy S, A M, Selvaraj D, Khalaf OI, Abdulsahib GM (2023) A Novel partial sequence technique based Chaotic biogeography optimization for PAPR reduction in eneralized frequency division multiplexing waveform. Heliyon 9(9):e19451.

22. Cheng H, Li X (2000) Partial encryption of compressed images and videos. EEE Trans Signal Process 48(8):2439–2451.
23. Rodrigues J, Puech W, Bors A (2006) Selective encryption of human skin in jpeg images. In: In 2006 International conference on image processing. IEEE, pp 1981–1984.
24. Ali R, Manikandan A, Xu J (2023) A novel framework of adaptive fuzzy-GLCM segmentation and Fuzzy with capsules network (F-CapsNet) classifcation. Neural Comput Applic.
25. Kumar, B. Sakthi, and R. Revathi. "An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network." *Journal of Engineering and Applied Science* 71, no. 1 (2024): 41.
26. Wang, Zhaoshun, and Mujahid Tabassum. "A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security." *Computers, Materials & Continua* 78, no. 3 (2024).
27. Bahache, Anwar Noureddine, Noureddine Chikouche, and Sedat Akleylek. "Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework." *Internet of Things* (2024): 101200.
28. Rajeshkumar, K., S. Dhanasekaran, and V. Vasudevan. "A novel three-factor authentication and optimal mapreduce frameworks for secure medical big data transmission over the cloud with shaxecc." *Multimedia Tools and Applications* (2024): 1-29.
29. Rana, Muhammad, Quazi Mamun, and Rafiqul Islam. "Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers." *Sensors* 23, no. 18 (2023): 7678.
30. Desoky, Abdelrahman, Hany Ammar, Gamal Fahmy, Shaker El-Sappagh, Abdeltawab Hendawi, and Sameh Hassanien Basha. "A novel keyless cryptosystem based on Latin square and cognitive artificial intelligence for blockchain and covert communications." *Int. J. Applied Cryptography* 4, no. 3/4 (2023): 219-237.
31. Han, Juhyeng, Insu Yun, Seongmin Kim, Taesoo Kim, Sooel Son, and Dongsu Han. "Scalable and secure virtualization of hsm with scaletrust." *IEEE/ACM Transactions on Networking* (2022).
32. Dua, Mohit, Drishti Makhija, Pilla Yamini Lakshmi Manasa, and Prashant Mishra. "3D chaotic map-cosine transformation based approach to video encryption and decryption." *Open Computer Science* 12, no. 1 (2022): 37-56.
33. Noura, Hassan N., Reem Melki, Ali Chehab, and Javier Hernandez Fernandez. "Efficient and robust data availability solution for hybrid PLC/RF systems." *Computer Networks* 185 (2021): 107675.
34. Cambou, Bertrand, David Hély, and Sareh Assiri. "Cryptography with analog scheme using memristors." *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 16, no. 4 (2020): 1-30.
35. Sengupta, Jayasree, Sushmita Ruj, and Sipra Das Bit. "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT." *Journal of network and computer applications* 149 (2020): 102481.
36. Zhu, Yuxuan, Bertrand Cambou, David Hely, and Sareh Assiri. "Extended protocol using keyless encryption based on memristors." In *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, pp. 494-510. Springer International Publishing, 2020.
37. Hu, XiaoKang, Jian Li, Changzheng Wei, Weigang Li, Xin Zeng, Ping Yu, and Haibing Guan. "STYX: A hierarchical key management system for elastic content delivery networks on public clouds." *IEEE Transactions on Dependable and Secure Computing* 18, no. 2 (2019): 843-857.

38. Wang, Zhu, Yan Yao, Xiaojun Tong, Qinghua Luo, and Xiangyu Chen. "Dynamically reconfigurable encryption and decryption system design for the internet of things information security." *Sensors* 19, no. 1 (2019): 143.