International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0368

e ISSN: 2584-2854
Volume: 02
Issue: 08 August 2024
Page No: 2543-2552

Concealing And Encrypting: Dual Approaches to Data Security in The Digital Age

Ananya Mishra[1], *Madhav Aggarwal*[2], *Akshat Tiwari*[3]
[1,2,3]*Department of Computer Science, MRU, Faridabad-Haryana, 221010, India.*
Emails: *mishraananya103@gmail.com*[1], *madhavaggarwal286@gmail.com*[2], *akshattiwari2323@gmail.com*[3]

Abstract

Ensuring data security is a paramount concern in the contemporary digital landscape, given the rapid advancements in internet technology leading to a substantial surge in online transfer of both textual and multimedia information. The current modes of communication lack robust security measures, making data vulnerable to unauthorized access during transmission. Recognizing the critical importance of safeguarding electronic data, both public and private sectors employ various procedures and methods. Among the prominent technologies employed for data security are cryptography and steganography. Cryptography involves the art of encrypting information to hide its readable and significant contents, whereas steganography is a technique used to conceal data within a cover media, effectively masking the very existence of the data. It is imperative for organizations to adopt and integrate these security technologies to mitigate the risks associated with unauthorized data access and ensure the integrity of sensitive information.

Keywords: *Data Security; Steganography; Cryptography; Masking;*

1. Introduction

The proliferation of information shared on electronic platforms has witnessed a significant upswing in recent years. With technological advancements, data transmitted through insecure channels faces an escalating risk. It is imperative to ensure that data remains inaccessible to unauthorized entities, fortified against illicit access, and immune to unlawful tampering. Consequently, maintaining the security and confidentiality of transmitted data becomes a critical necessity. Various data security methods, such as Steganography and Cryptography, serve to meet these imperatives. Cryptography can be broadly categorized into two types: symmetric and asymmetric. Symmetric encryption involves both the transmitter and the receiver using the same key, while asymmetric-key cryptography employs two distinct keys—a public key accessible to everyone and a private key known exclusively to the designated recipient. Despite conveying secret data in an unintelligible manner through cryptography, the recipient is aware of its existence. Steganography, on the other hand, prevents unintended recipients from even detecting the presence of secret data by concealing it within other data. This makes Steganography advantageous, particularly in situations where using cryptography might be deemed unsafe or illegal. Unlike cryptography, which primarily secures the message being transmitted over the network, Steganography safeguards both the conversing parties and the message itself. Although various secure techniques are available, technological advancements can weaken these methods over time, necessitating continuous improvement for more effective and secure data transfer.

2. Literature Review

Cryptography plays a crucial role in enhancing data security within the realm of cloud computing. The utilization of cloud storage not only alleviates users' storage burdens but also provides them with convenient access, solidifying its significance as a pivotal cloud service. However, challenges to cloud data security arise from potential intrusions.

Additionally, concerns linger over the trustworthiness of various data management operations, including storage, backup, migration, deletion, update, search, query, and access, as they may not be fully trusted by the data owners. Consequently, the authorization of cloud data processes and the protection of data emerge as compelling research areas. Data security model is shown in Figure 1.

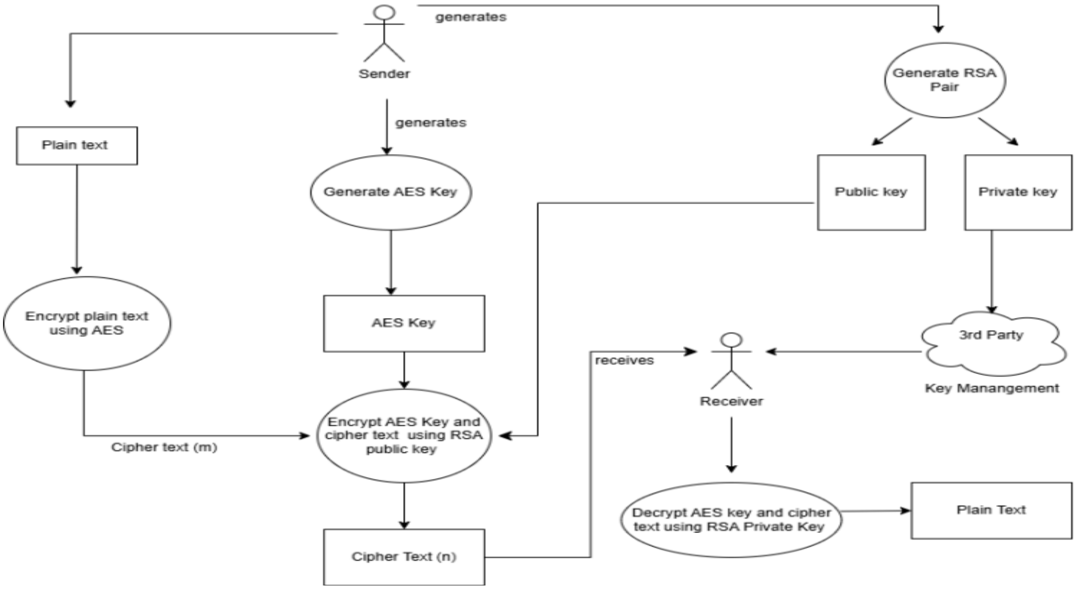

Figure 1 **Data Security Model**

The articles "Secure Independent-update Concise-expression Access Control for Video on Demand in Cloud" by He et al., and "Cryptography-Based Secure Data Storage and Sharing Using HEVC and Public Clouds" by Usman, Jan, and He, propose innovative schemes leveraging Attribute-Based Encryption to ensure flexible and efficient authentication and authorization for Video on Demand (VoD) services. Addressing the need for secure, lightweight, energy-efficient, and robust solutions, Li et al. propose an intelligent cryptography approach named Security-Aware Efficient Distributed Storage (SA-EDS) model in "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing." This model restricts direct access to partial data by cloud service operators. Similarly, Hu et al. tackle the challenge of outsourced image reconstruction and identity authentication in "A Compressive Sensing Based Outsourcing of Image Storage and Identity Authentication Service in Cloud." Peng et al. contribute to overcoming the limitations of Secure Approximate k-Nearest Neighbor (SANN) queries from encrypted databases in "A Reusable and Single-interactive Model for Secure Approximate k-Nearest Neighbor Query in Cloud." Their model ensures efficiency, recoverability, and non-distinguishability in processing such queries without decrypting the data. Additionally, Peng et al. address privacy concerns in Location-Based Services (LBS) over the cloud in "Collaborative Trajectory Scheme in Location-based Services." Each of these studies contributes to the ongoing discourse on bolstering cloud data security, privacy, and trust, which are pivotal for the success of cloud computing. [1] We have explored the fundamental concepts, features, and goals of diverse cryptographic algorithms. Our discussion has emphasized the integral role of embedded frameworks within most communication systems, underscoring their attractiveness as potential platforms for implementing cryptographic calculations. Notably, past executions of arithmeticintensive cryptographic algorithms suggest their capability to attain satisfactory performance even on constrained platforms and embedded processors, despite the inherent challenges. Consequently, we posit that the ongoing research focus on designing and implementing efficient cryptographic algorithms in embedded systems will persist as a prominent and active area of exploration. [2] Machine learning (ML) and deep learning (DL) have recently sparked considerable interest and garnered unprecedented community attention. The increasing integration of online activities and digital lifestyles is shaping how individuals learn and operate, but it also exposes them to significant security concerns. Safeguarding sensitive information, documents, networks, and machine-connected devices from unwarranted cyber threats poses a formidable challenge. To address this, a robust cybersecurity defense is imperative. In seeking solutions, contemporary innovations such as machine learning and deep learning are applied to counteract cyber threats. This paper explores the challenges and advantages associated with using ML/DL and provides recommendations for research directions in the application of machine learning and deep learning to enhance cybersecurity. [3] Data transmission in network security stands as a critical concern in contemporary communication. The proposed method's outcomes are delineated herein, showcasing its potential for achieving heightened security. The robust expansion of information communication has notably facilitated more accessible data transmission. The current focus within the realm of steganography and steganalysis reflects a growing interest, especially in hiding secret messages within images using innovative algorithms. To ensure the security of modified secret data, a dual approach involving encryption and steganography is employed. The combination of these methods enhances overall data security. Steganography is utilized for data concealment, while cryptography serves to encrypt the data. This tandem approach involves hiding encrypted data within a cover image, producing a stego image. The LSB method demonstrates superior performance, particularly in image files requiring elevated resolution and diverse color representations. It is also effective with audio files featuring distinct sounds and higher bit rates. Upon reception, the data is initially extracted, but it remains in an encrypted form, necessitating decryption using a key known solely to the receiver. This two-layer protection ensures secure transmission, employing the RSA algorithm for cryptography and LSB modification for steganography. Digital signatures, founded on public key encryption, further fortify the security of image files. The private key encrypts a hashed version of the image, generating a unique signature accessible only to the entity with knowledge of the private key. The integration of steganography with cryptography enhances message authentication through the use of digital signatures. Steganography ensures the hiding of files, providing high-security levels for data transmission. The method considers hiding messages in the LSB of the blue color of each pixel in the cover image. The signature image's encrypted information is then embedded into the cover image, creating a stego image sent to the receiver. This approach supports the concept of digital signatures by extracting the encrypted signature image information at the receiver end. Using the sender's public key, the original image information is decrypted. The retrieved signature is compared with the sender's stored scanned signature, offering support for message integrity, authentication, and non-repudiation. The paper demonstrates the fusion of steganography with digital signatures to enhance secrecy and safety in internet data transmission. Future work may explore more sophisticated algorithms with minimal stego object modification for even more secure data transmission. Additionally, incorporating support for error detection and correction could further enhance the overall capability for improved message authentication, privacy, security, and integrity in e-world communication.[4] Cryptography plays a pivotal role in accomplishing fundamental security goals, encompassing authentication, integrity, confidentiality, and non-repudiation. The fulfillment of cryptographic objectives is reliant on the evolution of algorithms. The primary role of cryptography is to furnish trustworthy, robust, and reliable security for networks and data. This paper delves into cryptographic research, exploring the functionality of various algorithms designed to meet diverse security objectives. The integration of cryptography into IT and business plans remains essential to uphold and ensure a satisfactory level of privacy for personal, financial, medical, and e-commerce data. [5] This chapter has explored diverse cryptographic methods aimed at safeguarding data during usage, storage, and transit. We anticipate these techniques to play a vital role as security becomes an imperative requirement for managing sensitive big data within the big data ecosystem. The purpose of this discussion is to enhance understanding regarding the latest technologies and safeguards related to big data security. We posit that fostering improved communication and closer collaboration between the communities of data science and cryptography is essential to facilitate the evolution of big data processing in the future.[6] This study challenges the misconception that the availability and pricing of spot instances are significantly affected by bidding. It is illustrated that the availability, cost, and revocation rate of spot instances remain relatively consistent across a wide range of bids, irrespective of spot pricing history. Consequently, we argue that users should allocate less emphasis on optimizing bidding strategies and, instead, focus more on adapting programs to efficiently identify and transition to the most cost-effective resources.[7] The latest paradigm in data communication is emerging through cloud computing. Various cryptographic algorithms, including AES, DES, and Triple DES for symmetric-key cryptography, are available for data encryption within cloud architecture. Asymmetric cryptography, utilizing a pair of keys (Public and Private Keys) such as RSA, ECC, and Elgamal, is employed for encryption and decryption. These asymmetric cryptosystems are commonly used for key management and are notably less vulnerable to attacks. Among public-key cryptosystems, RSA stands out, utilizing a significantly larger key size compared to ECC. This study endeavors to assess the effectiveness of ECC in comparison. [8] DNA Cryptography has now emerged as a robust method for ensuring data security due to its meticulously calculated key generation and decryption times, making the deciphering of encoded data practically infeasible. As a result, it stands as a primary choice for safeguarding data and information in the realm of cybersecurity research. The research conducted in this study is comprehensive, offering valuable data that will significantly assist researchers in their future endeavors in this domain. The modules for key generation, encryption, and decryption presented in this work will undeniably facilitate the implementation of cryptographic techniques in forthcoming studies. This current research contributes to the utilization of DNA steganography and cryptography technologies.[9] The primary application of big data lies in the analysis of extensive datasets to reveal novel insights and generate added value. Thus, the pivotal component of big data technology is the data mining and analysis algorithm, characterized by the 3Vs—Volume, Variety, and Velocity. Ensuring big data security is paramount, as it instills confidence in individuals to willingly contribute their data for analytics, given the assurance of the accuracy of newly discovered knowledge. Consequently, cryptography systems designed for big data security should possess two crucial characteristics: 1) Cryptography algorithms must exhibit excellent scalability and efficiency to effectively manage large datasets. 2) Cryptography technology should fulfill the requirements of security analysis for big data, capable of not only analyzing and mining large datasets but also safeguarding the security of big data and preserving user privacy. [10] A new approach to encrypting and decrypting confidential messages was proposed, tested, and implemented. The experimental findings revealed the following aspects:

- The devised method for data cryptography can be considered symmetric.
- Different messages can be encrypted and

decrypted utilizing the same base color image. Moreover, the size of an encrypted message can surpass that of an image.

- The substance of the communication does not influence the encryption process.
- The security level is notably high due to the difficulty in determining the source image.
- The proposed method is simple, devoid of any arithmetic or logical operations, and does not necessitate additional data structures like S-boxes.
- In comparison to the DES method, the proposed strategy exhibits heightened efficiency. [11]

Initially, the paragraph delves into the definition of cyberspace, the characteristics of cyberspace data, and the associated security concerns. Subsequently, it constructs a framework aimed at ensuring the security of cyberspace data. The framework is rooted in cryptography, forming a reference model for cyberspace data security. This model explores the foundational methodology and essential technology for safeguarding cyberspace data throughout its entire lifecycle, encompassing data generation, transmission, storage, usage, and destruction. This essay adopts a technological framework perspective to scrutinize and contribute constructively to the issue of cyberspace data security.[12] The prevailing viewpoint asserts that information security will play a pivotal role not only in the future IT landscape but also in various systems where electronic data exchange occurs. Cryptology stands out as the primary tool for ensuring information security. Cryptographic primitives are instrumental not only in safeguarding data communication but also in guaranteeing the safety and reliability of the overall system. In certain applications involving automated control based on data communication among diverse devices, the latter often takes precedence. Cryptology encompasses two algorithm types: symmetric and asymmetric (public-key) algorithms. This chapter extensively covers symmetric key cryptography, along with its subsets, block ciphers, and stream ciphers. Additionally, we provide concise overviews of two widely used algorithms in the industry: DES and AES. Our focus will be on their unique properties from an implementation perspective. Comprehensive attention will be devoted to the software and hardware implementations of DES, 3-DES, and AES, along with an exploration of the various modes of operation of block ciphers, enabling their utilization as stream ciphers.[13] At the core of network security lies cryptography, serving as a fundamental element. Ensuring privacy and protecting sensitive information becomes especially crucial in the development of systems or applications involving network connectivity. The application of cryptography extends to databases, given the significance of data in IoT devices. Encrypting substantial amounts of information is imperative to prevent interception and tampering. Despite its frequent application, cryptography often goes unnoticed. This paper delves into the utilization of cryptography within databases, offering recommendations to enhance security and privacy measures.[14] The term "Internet of Health Things" (IoHT) denotes individually identifiable devices interconnected through the Internet for communication. IoHT encounters various challenges, with cybersecurity standing out as a pivotal aspect in the realm of intelligent health monitoring and enhancement systems. Ciphertext-policy weighted attribute-based encryption (CP-WABE), a widely used security method for achieving fine-grained access control, holds the potential to ensure data security in the IoT. However, existing issues such as inflexibility, limited computational capacity, and inadequate storage efficiency are noteworthy. To address these concerns, we propose a novel approach for expressing access policies, employing 0-1 coding technology. Through this methodology, a versatile and efficient CP-WABE is constructed specifically for IoHT applications.[15] Let's explore the challenge of maintaining the confidentiality of the database's data, not just the query itself. The traditional approach to ensuring data confidentiality is encryption. However, when users encrypt the data stored in a database to protect it from unauthorized access, the functionality of database queries becomes limited to basic storage and retrieval operations, making the encrypted data less versatile. A significant challenge arises when the database is tasked with responding to queries involving multiple encrypted fields, as it appears that the database must decrypt the data before evaluating such queries. However, a method called homomorphic encryption offers a solution to this concern. The fundamental concept is to encrypt each data unit, such as a bit, without the database being aware of the encryption key. The database conducts logical operations on the encrypted bits as per the query, yielding the encrypted result of the query, which is then returned. This allows the database to perform operations on the encrypted data without possessing access to the decryption key. Double layer security is shown in Figure 2.

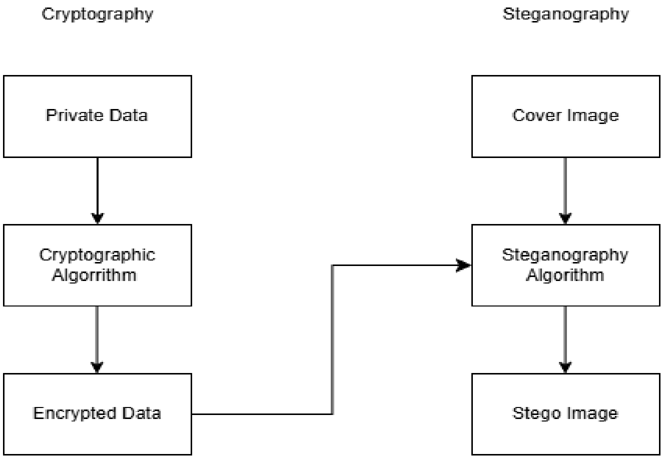

Figure 2 Double Layer Security

Achieving non-interactive computation with encrypted data would be possible if a probabilistic bit-encryption scheme homomorphic concerning a complete set of logical operations (like the NAND gate or EXOR and AND gates) could be developed. This remains an intriguing open problem in cryptography, with current solutions requiring substantial communication for evaluating each logical gate. Conceivably, both the query and the data could be concealed from the database by utilizing a universal circuit that takes a description of a circuit as its input. The Internet of Things (IoT) has significantly influenced our daily lives, connecting IoT devices with the physical world through the Internet. IoT applications use the cloud to store and provide ubiquitous access to collected data, raising security and privacy concerns, including the risk of data breaches. Existing cryptographic solutions, due to their significant computational overhead, are unsuitable for IoT devices with limited resources. In response to these concerns, we propose a data protection scheme that stores encrypted IoT data in the cloud while enabling query processing over the encrypted data. Our proposed scheme features an innovative encrypted data-sharing plan based on the Boneh-Goh-Nissim (BGN) cryptosystem, incorporating denial capabilities and in-situ key updates. To assess the feasibility of implementing the proposed scheme on IoT devices with limited resources, extensive experiments are conducted on real datasets. The results demonstrate the viability and capacity of our strategy to provide a high level of security. Furthermore, the findings indicate that, compared to the best-performing scheme in the current state of the art, our scheme significantly reduces energy, storage, and computation overheads.[17] The Internet of Health Things (IoHT) pertains to distinctively identifiable devices interconnected through the Internet, enabling communication among them. IoHT encounters numerous challenges, with cybersecurity standing out as a crucial element in smart health monitoring and enhancement systems. Ciphertext-policy weighted attribute-based encryption (CP-WABE), a widely utilized security method for achieving precise access control, holds promise for ensuring data security in the IoT. However, persisting issues, including inflexibility, limited computational capacity, and insufficient storage efficiency, remain noteworthy when assessing its attributes. To address these challenges, we propose a novel approach to articulate access policies utilizing 0-1 coding technology. Through this innovative methodology, a flexible and efficient CP-WABE is devised specifically for IoHT applications.[18] The utilization of the golden ratio holds significance in secret key generation and secure cryptographic applications, and our study introduces an efficient method for its computation. Despite the availability of various cipher-based encryption techniques, their sluggish computation speeds have hindered their effectiveness in countering the growing threats to security. Recently, golden cryptography, a novel encryption approach incorporating golden ratio calculations, has emerged. Our proposed method leverages the advanced properties of diophantine equations in computations, deviating from previous techniques that relied on the well-known Fibonacci sequence method for golden ratio computation. We initially established these mathematical properties and outlined our proposed approach. Subsequently, we experimentally computed the golden ratio with infinite precision using our suggested method. Finally, we evaluated our approach by comparing the computational results with the widely used Fibonacci sequence method. The efficacy of our proposed golden ratio method was demonstrated in terms of computational speed and accuracy. Future investigations will explore how the expedited cryptographic algorithms resulting from this discovery may impact the ability to withstand security breaches. Examining how our faster golden ratio computation method can enhance cryptographic security by establishing practical secret keys for promptly thwarting potential information security breaches would be particularly intriguing. [19] The comprehensive cryptographic accelerator introduced in this study plays a crucial role in fortifying the security of dynamic data within embedded systems. To mitigate the risks of sensitive data leaks and tampering assaults resulting from off-chip physical attacks, the accelerator design incorporates a four-parallel AES-GCM hardware structure, ensuring authenticated encryption. This design contributes to enhancing the trustworthiness of the embedded system by safeguarding data integrity and confidentiality, effectively generating an integrity digital signature for security verification. Through an assessment of processing efficiency and performance overhead, the results indicate that the cryptographic accelerator excels in encryption processing efficiency while maintaining minimal performance overhead. Specifically, on standard 8-KB I/D-Caches, the average performance overhead diminishes to as low as 2.6 per cent.[20] We offer a comprehensive examination of data security and privacy preservation within cloud storage systems in this article. Primarily, the enduring popularity of cloud computing and storage is undeniable, driven by its remarkable performance in the digital economy, business digital transformation, the Internet of Things, and various other domains. The analysis encompasses eight key aspects of data security in cloud storage systems: data confidentiality, data integrity, data availability, fine-grained access control, secure data sharing in dynamic groups, leakage resistance, fully deleted data, and privacy protection. Subsequently, we delve into the fundamentals of IBE (Identity-Based Encryption), ABE (Attribute-Based Encryption), homomorphic encryption, searchable encryption, and elucidate the future research trajectory involving innovative encryption models. The article also outlines technologies and methodologies for data protection that align with the aforementioned security criteria.[21] We introduce an innovative two-factor data security protection mechanism designed for cloud storage systems. This mechanism mandates the recipient to utilize both their secret key and a security device for accessing encrypted data. Consequently, only the data sender possessing knowledge of the receiver's identity is authorized to encrypt the data. With our approach, the cloud server can promptly update the pertinent ciphertext without the data owner's awareness once the device is revoked. This dual-factor authentication not only enhances data confidentiality but also endows the system with device revocability. Additionally, we provide an analysis of the system's efficiency and a security proof.[22] Since applied cryptography has advanced significantly over the past few decades, cryptographic systems are becoming increasingly complicated and demanding greater processing power. In order to generally secure the security of data transfer, it is also crucial to use the right protocols for the transmission channels. In this situation, quantum cryptography, which is based on subatomic events, resolves the channel security issue and creates an entirely secure data transmission system.[23] The encryption algorithm continues to play a crucial role in ensuring communication safety. Our research involved the implementation of widely used encryption methods, including AES, DES, and RSA algorithms. The experimental results, based on the analysis of text files, led to the observation that the AES algorithm exhibits the shortest encryption time, while the RSA algorithm demonstrates the longest. Furthermore, our findings indicated that the AES algorithm's decryption outperforms that of other algorithms. Analyzing these results, it is evident that the AES algorithm significantly outperforms the DES and RSA algorithms. Subsequently, we plan to compare and analyze existing cryptographic algorithms like AES, DES, and RSA using audio and image data as input, with a focus on reducing encryption and decryption times. [24] The section discusses various categories of information security issues, broadly falling under physical security, communication security, and operational security (encompassing database security, operational security, and computer viruses). Cryptography, or the art of transforming information using a key to make it unintelligible to those without the key, is then introduced as a method for addressing various computer security concerns. The text provides a detailed exploration of different types of cryptosystems, detailing their classifications based on capability, number of keys, and application methods for securing information. In a symmetric cryptosystem, the encryption key and the decryption key are identical, whereas in an asymmetric cryptosystem, they are distinct. The section also acknowledges that various types of attacks can impact cryptosystems, and cryptanalysis is presented as the method for attacking a cryptosystem.[25]

Conclusion

This essay delves into various methods employed for data protection, each with its own set of advantages and drawbacks, and their suitability varies across different application domains. Common parametric needs include capacity, security, robustness, and imperceptibility, and different methodologies cater to these needs to varying degrees. Some approaches prioritize security over others, while some excel in hiding more data. Certain tactics exhibit greater resistance to specific types of attacks, while others may be more delicate in this regard. While some procedures are basic but lack the same level of security as more sophisticated methods, others are advanced yet maintain a high level of security. In many cases, fulfilling certain criteria might come at the expense of others. Employing a combination of strategies becomes a viable option to optimize the fulfillment of parametric needs, ensuring data security. Despite several secure techniques being available, technological advancements often render these methods less effective, necessitating continuous improvement for more robust and secure data transfer.

References

[1]. Reyad, O. (2018). Cryptography and data security: An introduction. *the International Journal of Computer Science and Security*.

[2]. Wollinger, T., Guajardo, J., & Paar, C. (2003). Cryptography in embedded systems: An overview. Proc. Embedded World, 735-744.

[3]. Kaushik Dushyant, Garg Muskan, Annu, Ankur Gupta, Sabyasachi Pramanik, "Utilizing Machine Learning and Deep Learning in Cybersecurity: An Innovative Approach", Cyber Security and Digital Forensics, pp.271, 2022.

[4]. Pramanik, Sabyasachi, Samir Kumar Bandyopadhyay, and Ramkrishna Ghosh. "Signature image hiding in the colour image using steganography and cryptography based on digital signature concepts." 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 2020.

[5]. Qadir, A. M., & Varol, N. (2019, June). A review paper on cryptography. In 2019 7th international symposium on digital forensics and Security (ISDFS) (pp. 1-6). IEEE.

[6]. Hamlin, A., Schear, N., Shen, E., Varia, M., Yakoubov, S., & Yerukhimovich, A. (2016). Cryptography for Big Data Security. IACR

Cryptol. ePrint Arch., 2016, 12.

[7]. Sharma, G., & Kalra, S. (2016, August). A novel scheme for data security in cloud computing using quantum cryptography. In Proceedings of the International Conference on Advances in Information Communication Technology & Computing (pp. 1-6).

[8]. Khan, I. A., & Qazi, R. (2019). Data security in cloud computing using elliptic curve cryptography. International Journal of Computing and Communication Networks, 1(1), 46-52

[9]. Das, A., Sarma, S. K., & Deka, S. (2021). Data security with DNA cryptography. In Transactions on Engineering Technologies: World Congress on Engineering 2019 (pp. 159-173). Springer Singapore.

[10]. Xiaosong, Z. (2015). Research of cryptography technologies for big data security. *Journal of Information Security Research*, *1*(3), 238.

[11]. Alqad, Z., Oraiqat, M., Almujafet, H., Al-Saleh, S., Al Husban, H., & Al-Rimawi, S. (2019). A new approach for data cryptography. International Journal of Computer Science and Mobile Computing, 8(9), 30-48.

[12]. Yang, T., & Yu, B. (2014, July). Study of cryptography-based cyberspace data security. In Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[13]. Kumar, S., & Wollinger, T. (2006). Fundamentals of symmetric cryptography. Embedded Security in Cars: Securing Current and Future Automotive IT Applications, 125-143.

[14]. Xu, H., Thakur, K., Kamruzzaman, A. S., & Ali, M. L. (2021, April). Applications of cryptography in database: a review. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-6). IEEE.

[15]. Tyagi, S. S. (2021, February). Secure data storage in cloud using encryption algorithm. In 2021 third international conference on intelligent communication technologies and virtual mobile networks (ICICV) (pp. 136-141). IEEE.

[16]. Maurer, U. (2004, June). The role of cryptography in database security. In Proceedings of the 2004 ACM SIGMOD international conference on Management of data (pp. 5-10).

[17]. Halder, S., & Conti, M. (2021). Crypsh: A novel iot data protection scheme based on bin cryptosystem. IEEE Transactions on Cloud Computing, 10(4), 2437-2450.

[18]. Tyagi, S. S. (2021, February). Secure data storage in cloud using encryption algorithm. In 2021 third international conference on intelligent communication technologies and virtual mobile networks (ICICV) (pp. 136-141). IEEE.

[19]. Overmars, A., & Venkatraman, S. (2018). An efficient golden ratio method for secure cryptographic applications. Mathematical and Computational Applications, 23(4), 58.

[20]. Zhang, Z., Wang, X., Hao, Q., Xu, D., Zhang, J., Liu, J., & Ma, J. (2021). High-efficiency parallel cryptographic accelerator for real-time guaranteeing dynamic data security in embedded systems. Micromachines, 12(5), 560.

[21]. Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.

[22]. Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2015). Two-factor data security protection mechanism for cloud storage system. IEEE Transactions on Computers, 65(6), 1992-2004.

[23]. Cangea, O., Oprina, C. S., & Dima, M. O. (2016, June). Implementing quantum cryptography algorithms for data security. In 2016 8th international conference on

electronics, computers and artificial intelligence (ECAI) (pp. 1-6). IEEE.

[24]. Hossain, M. A., Hossain, M. B., Uddin, M. S., & Imtiaz, S. M. (2016). Performance analysis of different cryptography algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3).

[25]. Davida, G. I., & Desmedt, Y. (1990). Cryptography based data security. In Advances in computers (Vol. 30, pp. 171-222). Elsevier.