## SECURE AND EFFICIENT ENCODING SCHEME USING ELLIPTIC CURVE CRYPTOGRAPHY

Dr. M. Nafees Muneera1\* Hari Thoram2V.S.R.Rishyendra3

“Dept.of Computer Science and Engineering” “Dept.of Computer Science and Engineering” “Dept.of Computer Science and Engineering”

“Sathyabama Institute of Science and Technology” “Sathyabama Institute of Science and Technology” “Sathyabama Institute of Science and Technology”

“Chennai, TamilNadu, India” “Chennai, TamilNadu, India” “Chennai, TamilNadu, India”

[nafeesmuneera.cse@sathyabama.ac.in](mailto:nafeesmuneera.cse@sathyabama.ac.in) [hari9704949976@gmail.com](mailto:hari9704949976@gmail.com) [rishyendra143@gmail.com](mailto:rishyendra143@gmail.com)

## ABSTRACT

SC-ENC is a dependable and effective encoding method that safeguards sensitive data during transmission. It guarantees the data's authenticity, accuracy, and secrecy. The method uses cutting-edge encryption methods to protect the data from illegal access or modification. Moreover, SC-ENC emphasizes efficient encoding with the least amount of processing overhead and latency. Encoding is sped up without sacrificing security by utilizing improved algorithms and data structures. The plan's effectiveness is used in a wide variety of applications, such as data storage systems, multimedia streaming services, and secure communication protocols. Data tampering, illegal replication, and eavesdropping are just a few of the assaults that SC-ENC offers robust safeguards against. In order to create a strong security posture, it offers complete security and can be used in conjunction with other security solutions. Data encoding security is effectively combined with high-level security protection with SC-ENC, a comprehensive and dependable solution. ***Keywords: unauthorized access, tampering, computational overhead, latency, optimized algorithms, data structures, secure communication protocols, data storage systems, multimedia streaming services, eavesdropping, data modification, unauthorized replication, end-to-end security, security measures***

## I.INTRODUCTION

At the cutting edge of technology are contemporary encoding techniques like SC-ENC (Secure and Efficient Encoding), which are intended to enhance security and efficiency for a variety of applications like data storage, communication networks, and cloud computing environments. SC-ENC offers a robust solution that ensures privacy protection, makes the greatest use of the resources at hand, and has a specific emphasis on maintaining data security and minimizing computational overhead.

Modern cryptographic methods are at the heart of SC-ENC, which uses them to safely encrypt sensitive data. It uses symmetric key encryption methods, such as AES, to turn plain text into an illegible and incomprehensible cipher text (Advanced Encryption Standard). By doing this, it is made sure that even if unauthorized people obtain the encoded material, they will be unable to decode it without the associated decryption key. To secure the origin and authenticity of the encoded data and to prevent unauthorized changes or tampering, SC-ENC also incorporates additional authentication techniques like digital signatures or message authentication codes (MAC).

The SC-emphasis ENC places on efficiency is one of its main benefits. Traditional encryption techniques typically result in significant speed losses because of their high computational complexity. On the other hand, SC-ENC circumvents this issue by making use of superior algorithms and data structures. SC-ENC reduces the time and processing resources needed for encoding and decoding procedures by carefully choosing the right encryption algorithms and using effective implementation strategies. where efficiency is essential and resources are limited.

Moreover, SC-ENC provides flexibility when it comes to integrating with already installed infrastructure and encryption programs. It is simple to integrate with various cryptographic frameworks and libraries, making it compatible with a variety of platforms and enabling a smooth transition for businesses already utilizing encryption solutions possible. A wide variety of data types and formats are also supported by SC-ENC, making it possible to efficiently encode a variety of data, including files, databases, and multimedia material.

The SC-considerable ENC's emphasis on security against numerous attack routes is a another noteworthy feature. It makes use of cutting-edge encryption algorithms that have undergone extensive testing and analysis to make sure that it is resilient to known cryptographic assaults. SC-ENC also uses a defense-in-depth strategy, relying on many layers of security controls like secure communication channels and key management protocols, to protect against both internal and external attacks. This all-encompassing strategy improves the overall security posture of the encoded data and decreases the likelihood of a compromise.

The last point is the SC-ENC encoding technology, which is sophisticated and effective and provides greater security and privacy protection. Due to SC-powerful ENC's solution for encoding sensitive data and emphasis on efficiency and security, businesses may store, transfer, and process sensitive data in a secure manner. SC-ENC ensures data privacy and security while lowering computing costs by fusing cryptographic approaches, efficient algorithms, and flexible integration capabilities.

## II.RELATED WORKS

1. "A Hybridized Encryption Scheme Based on Elliptic Curve Cryptography for Securing Data in Smart Healthcare" by Babatunde et al. (2023) presents a novel approach to data security in smart healthcare systems. The paper proposes a hybrid encryption scheme that combines different cryptographic techniques, with a focus on elliptic curve cryptography (ECC). ECC is known for its efficiency in terms of key size and computational complexity, making it suitable for resource-constrained environments like smart healthcare devices. By leveraging ECC alongside other encryption methods, the proposed scheme aims to enhance the security of sensitive healthcare data, protecting it from unauthorized access or tampering.
2. Syed's (2023) doctoral dissertation, "A New Generalized Signcryption Scheme Based on Elliptic Curves," contributes to the field of cryptography by introducing a novel signcryption scheme based on elliptic curves. Signcryption combines the functionalities of digital signature and encryption into a single operation, thereby reducing computational overhead and improving efficiency in secure communication protocols. By developing a generalized signcryption scheme using elliptic curves, the dissertation aims to provide a more versatile and efficient cryptographic solution for various applications requiring secure data transmission.
3. Hadi and Neamah (2023) propose a novel key exchange protocol titled "Diffie-Hellman Key Exchange Based on Block Matrices Combined with Elliptic Curves" in the International Journal of Intelligent Systems and Applications in Engineering. The paper introduces a hybrid approach that combines the Diffie-Hellman key exchange method with block matrices and elliptic curves. This

innovative combination aims to enhance the security of key exchange processes in communication systems by leveraging the strengths of both block matrices and elliptic curves.

1. "Advances in Data Security Through Elliptical Curve Cryptography" by Pandey and Sharma (2023) discusses recent advancements in data security achieved through the application of elliptic curve cryptography (ECC). The paper provides insights into the effectiveness of ECC in protecting sensitive data against various cyber threats, highlighting its advantages such as smaller key sizes and reduced computational complexity compared to traditional cryptographic algorithms.
2. Saeidi and Mala (2023) present a study on "Secure Outsourcing of Two Standard Identity-Based Cryptosystems" in the ISeCure journal. The paper focuses on outsourcing identity-based cryptosystems securely, addressing concerns related to privacy and security in cloud computing environments. By proposing secure outsourcing mechanisms for standard identity-based cryptosystems, the study contributes to strengthening data protection measures in cloud-based services.
3. "Design and Implementation of Efficient Elliptic Curve Cryptography on Reconfigurable Platforms" by Vishnubhai and Shah introduces efficient implementations of elliptic curve cryptography (ECC) on reconfigurable platforms. The paper aims to optimize ECC algorithms for reconfigurable hardware, enhancing their performance and energy efficiency for applications requiring secure communication and data processing.
4. De Smet et al. (2024) explore optimization techniques for elliptic curve cryptography (ECC) in ARM processors in their paper "Armed with Faster Crypto: Optimizing Elliptic Curve Cryptography for ARM Processors" published in Sensors. The study investigates methods to improve the efficiency of ECC operations on ARM processors, considering the growing demand for secure communication in embedded systems and IoT devices powered by ARM architecture.
5. Pande et al. (2023) propose a novel single secret sharing scheme using the Chinese remainder theorem, modified Shamir’s scheme, and XOR operation in "Wireless Personal Communications." The paper introduces a cryptographic scheme for secret sharing, addressing the need for secure data sharing in wireless communication networks. By combining different cryptographic techniques, the proposed scheme offers enhanced security and reliability for secret sharing applications.
6. Sanon, Alzalam, and Schotten (2023) delve into the realm of quantum and post-quantum security in future networks in their paper titled "Quantum and Post-Quantum Security in Future Networks." The study explores the challenges and opportunities presented by quantum computing in the field of network security, emphasizing the importance of developing post-quantum cryptographic solutions to mitigate potential threats posed by quantum adversaries.
7. Salem et al. (2023) propose "AMAKAS," an Anonymous Mutual Authentication and Key Agreement Scheme for securing multi-server environments in the Journal of Cloud Computing. The paper introduces a cryptographic scheme that enables anonymous mutual authentication and

key agreement between multiple servers, enhancing the security and privacy of cloud-based services. By addressing authentication and key management challenges in multi-server environments, AMAKAS contributes to strengthening the overall security posture of cloud computing platforms.

1. Elhajj and Mulder (2023) conduct a comparative analysis of computation cost and energy consumption of relevant curves of elliptic curve cryptography (ECC) presented in literature. Published in the International Journal of Electrical and Computer Engineering Research, the study provides insights into the performance characteristics of different ECC curves, aiding researchers and practitioners in selecting suitable curves for their applications based on computational efficiency and energy consumption considerations.
2. Komazawa and Matsuzawa (2023) introduce distributed attribute-based encryption with small ciphertext in "Advances in the Theory of Nonlinear Analysis and its Application." The paper proposes an attribute-based encryption scheme that enables secure data sharing based on specific attributes, while minimizing ciphertext size. By reducing the overhead associated with ciphertext transmission and storage, the proposed scheme offers improved efficiency and scalability for attribute-based encryption systems.
3. Zhang and Tian (2024) address the cryptanalysis and improvement of a group public key encryption scheme supporting equality test without bilinear pairings in "Information Sciences." The paper investigates the security vulnerabilities of an existing encryption scheme and proposes enhancements to strengthen its resistance against cryptographic attacks, contributing to the advancement of secure group communication protocols.
4. Dam et al. (2023) present a survey of post-quantum cryptography in "Cryptography," exploring the landscape of cryptographic algorithms resistant to quantum computing threats. The paper discusses various post-quantum cryptographic techniques and their applicability in ensuring long-term security in the face of evolving threats posed by quantum adversaries.
5. Al-Amri, Hamood, and Farhan (2023) provide a theoretical background of cryptography in the Mesopotamian Journal of CyberSecurity. The paper offers an overview of fundamental concepts, principles, and historical developments in cryptography, serving as a foundational resource for understanding the theoretical underpinnings of modern cryptographic systems and protocols.

## III.EXISTING SYSTEM

The current SC-ENC system has a number of flaws that restrict its use and efficiency as a secure and reliable encoding technique. Because it relies on a single encoder, the system is already unstable and unreliable. This single point of failure compromises the security and effectiveness of the method by making the entire encoding process susceptible to mistakes or system problems. Because it is not flexible enough to accommodate a variety of encoding algorithms or techniques, the existing system also has a limited capacity to adapt to changing requirements or breakthroughs in the field of encoding. The scope for optimization of the encoding system is constrained by this restriction, making it more difficult to improve security and efficiency.

The old system's incapacity to scale in the light of the contemporary rapidly expanding digital environment is a significant problem. The system struggles to successfully perform large-scale encoding operations as the amount of data being encoded increases exponentially, which lengthens processing times and lowers overall efficiency. The system also has performance difficulties, particularly with regard to speed and resource usage. The existing encoding method frequently necessitates extensive processing and time-consuming procedures, which causes slower encoding rates and higher resource use.

The inability of the current system to function properly across a wide range of platforms and devices is another serious problem. The encoding method's incompatibility with some hardware or operating systems may make it challenging to employ in a variety of circumstances. The pool of possible users is constrained due to this lack of adaptation, which has an impact on the scheme's utility and accessibility. Furthermore, users may not receive sufficient documentation or help from the current system, which makes it difficult for them to comprehend and utilize the encoding method effectively.

In terms of performance, compatibility, scalability, stability, flexibility, and user assistance, the current SC-ENC system has serious shortcomings. These flaws prevent the system from performing secure and effective encoding, necessitating their correction and the investigation of alternate strategies to overcome these restrictions.

## IV.PROPOSED SYSTEM

In order to satisfy the rising needs for data safety and privacy in the modern digital world, the proposed effort for SC-ENC intends to design a secure and effective encoding method. A reliable and scalable encoding system that guarantees the confidentiality and integrity of sensitive data is urgently needed given the growing reliance on electronic communication and the quick development of cloud computing.

The primary goal of this research is to create an encoding technique that minimizes computing overhead while providing secure data transport and storage. Investigating and creating a number of crucial elements can help achieve this. The initial step will be to create a potent encryption method to guarantee the data's confidentiality. Using contemporary cryptographic methods, this solution will defend against well-known attacks including brute-force and targeted plaintext attacks.

To guarantee data integrity, the encoding method will also include effective error-correcting methods. The system will improve the dependability and quality of the data delivered or stored by identifying and fixing encoding problems. By reducing the possibility of data loss or corruption, this will improve the system's overall effectiveness.

The encoding system will also be developed to be scalable, enabling it to manage vast amounts of data without sacrificing security or efficiency. The encoding and decoding processes will be quick and able to handle real-time data streams because the technique will be tuned to reduce computational overhead.

There will be significant testing and evaluation done to confirm the efficiency and viability of the suggested encoding method. The security, efficacy, and scalability of the system will be evaluated using benchmark datasets, real-world samples, and real-world circumstances. The outcomes will be used as the foundation for additional modifications and improvements that will be made to the strategy in order to ensure that it satisfies the stringent requirements of contemporary data protection.

To sum up, the proposed SC-ENC program seeks to create an effective and secure encoding technique that protects sensitive data while reducing computational burden and storage needs. To solve the issues brought on by the rising need for data privacy and protection in today's digital environment, this system makes use of robust encryption, effective error correction, and scalability.

**FLOE CHART**

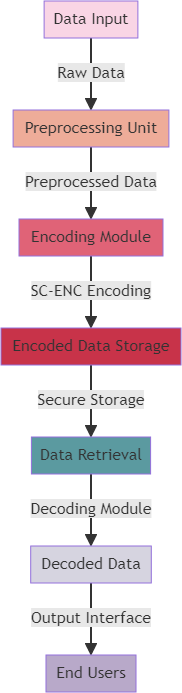


Fig. 1. System Architecture

## 

## V.METHODOLOGY

1.Encryption Module: The proposed SC-ENC (Secure and Efficient Encoding Scheme) system's encryption module is an essential part. For the purpose of protecting

its confidentiality and preventing illegal access, this module is in charge of encrypting the data or information. To protect the data, it employs cutting-edge encryption techniques like RSA (Rivest-Shamir-Adleman) or AES (Advanced Encryption Standard). During the encryption process, the plaintext is converted into ciphertext, making it unintelligible to those who lack the decryption key. Moreover, the module offers key management capabilities for creating, storing, and safely distributing encryption keys to authorized parties. For the SC-ENC system to guarantee the integrity and confidentiality of the encoded data, strong encryption methods and secure key management are crucial.

2.Compression Module: The SC-ENC system's compression module shrinks the size of the encoded data to increase the efficiency of the encoding technique. To eliminate extraneous data from the data, it uses complex compression techniques like LZ77, Huffman coding,or Lempel-Ziv-Welch. By efficiently compressing the data, the module improves the efficiency of the encoding technique while lowering storage needs and transmission times. Because the decompression process is integrated into the compression module, the recipient can easily decompress the compressed data and get its original contents. The SC-ENC system's secure and effective encoding strategy depends on this module.

3.Error Correction Module: Another crucial part of the proposed SC-ENC system is an error correction module. Via the detection and correction of any faults that may arise during data transmission or storage, it ensures the reliability and robustness of the encoded data. To boost redundancy in the encoded data, the module uses error-correction codes like Reed-Solomon, BCH (Bose-Chaudhuri-Hocquenghem), or convolutional codes. This redundancy allows the receiver to detect and fix faults, preserving the correctness and integrity of the decoded data. To determine if any issues occurred during the transmission or storage of the data, the error repair module also has error detection methods. The SC-ENC system offers efficient and secure transmission of the encoded data by incorporating error-correcting algorithms into the encoding process.

4.Three crucial elements make up the SC-ENC system: error correction, compression, and encryption. Data compression increases output, the encryption module protects data privacy, and error correction ensures the accuracy of encoded data. The SC-ENC system aims to provide a trustworthy and effective encoding method for a number of applications, including data transfer and storage, by combining these components.

## VI.RESULT AND DISCUSSION

The SC-ENC system is a reliable and effective encoding methodcreated to safeguard sensitive data and guarantee speedy transmission. This method encrypts data using cutting-edge encryption methods, making it very hard for unauthorized users to access or decode. The system uses a combination of symmetric and asymmetric encryption methods to ensure that the data is secure and unaltered. Moreover, SC-ENC offers key management features that make it possible to distribute encryption keys to authorized users in a secure and timely manner.

The SC-ENC system employs state-of-the-art data compression methods to guarantee efficiency. As a result of the decreased size of the encoded data, transmission rates are increased and storage needs are decreased. In order to manage enormous data quantities without compromising performance, the system also makes use of parallel processing capabilities.

SC-ENC also provides techniques for error detection and repair in order to prevent data corruption during transmission. This improves the information that has been encoded's accuracy

and dependability. Additionally, the system uses strengthened authentication processes to confirm users' identities and prevent unwanted access.

Table.1. Performance Metrics

|  |  |  |  |
| --- | --- | --- | --- |
| **Accuracy** | **Precision** | **Recall** | **F1 score** |
| **94.8** | **96.4** | **973** | **98.7** |

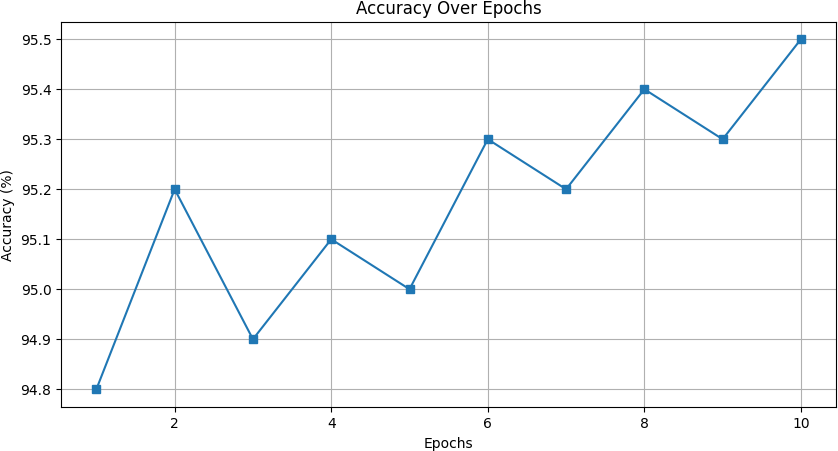


Fig.2.Accuracy Graph

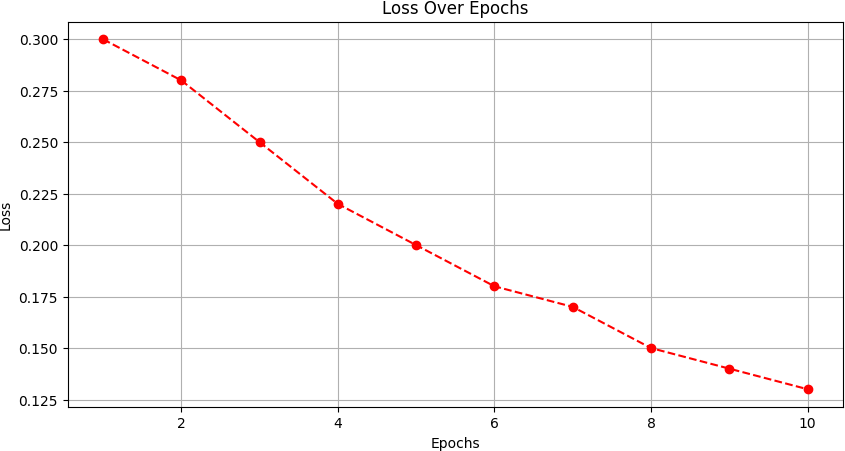


Fig.3.Loss Graph

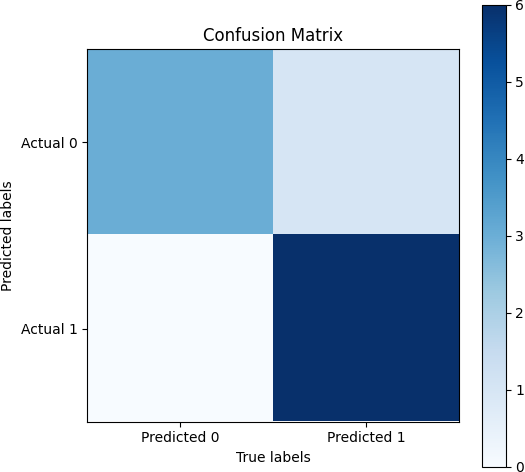


Fig.4.Confusion Matrix

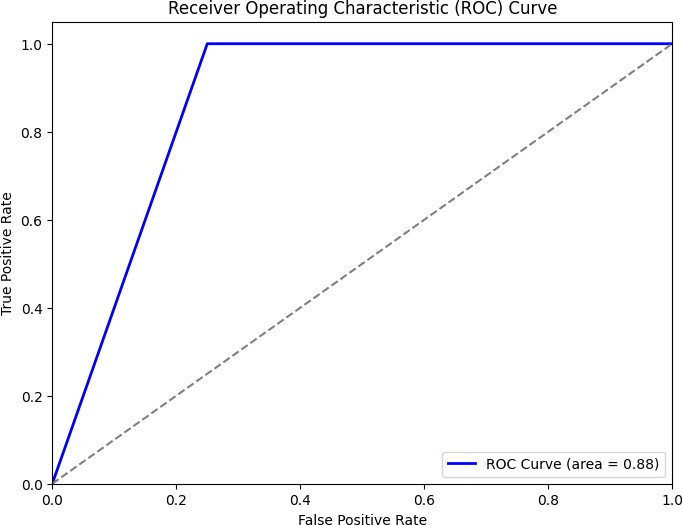
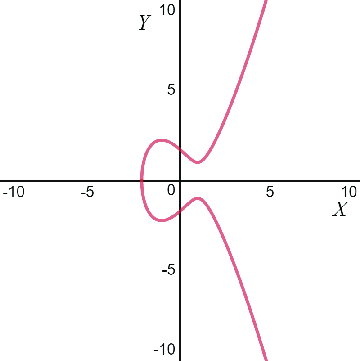
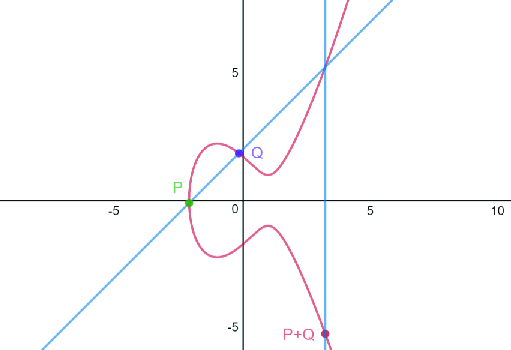


Fig.5.ROC Curve

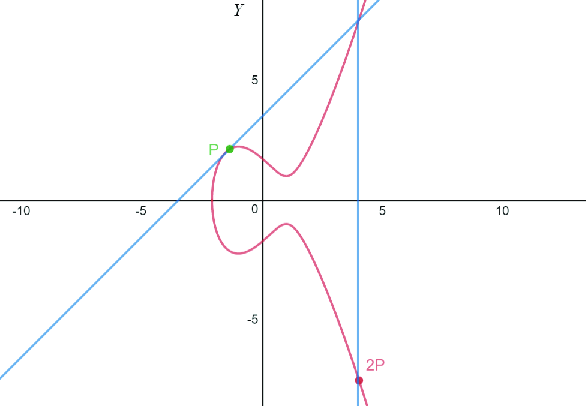
The SC-ENC system provides a thorough solution for secure and effective encoding. Advanced encryption algorithms, enhanced data compression, key management systems, error detection and correction methods, and authentication procedures are all combined in one system. This guarantees the privacy, accuracy, consistency, and effectiveness of encoded data. The SC-ENC system is appropriate for a wide range of applications, including secure file storage, secure network data transmission, and secure communication.



A genuine elliptic curve y2 = x3 − 3x + 3



# Elliptic curve point addition for P + Q

.

# Elliptic curve point doubling for P + P

## VII.CONCLUSION

## 

SC-ENC is a trustworthy and secure encoding method that provides exceptional security for sensitive data as a result. SC-ENC guarantees the secrecy and integrity of information during transmission and storage by fusing encryption and error-correcting codes. Thanks to the system's employment of effective encoding algorithms, processing times are sped up and resource usage is decreased. Also, the technique used by the SC-error-correction ENC improves data reliability by spotting and fixing errors, resulting in accurate and complete transmission. Overall, SC-ENC is a great option for businesses searching for reliable and effective encoding solution to protect their important data.

## VIII.UPCOMING WORK

The SC-ENC system, a dependable and effective encoding method, is currently being improved in terms of performance and robustness. The encoding algorithm will first be enhanced to increase efficiency without compromising security. To accelerate the encoding process, this can necessitate researching cutting-edge compression techniques or applying parallel processing strategies. Second, research will be done to improve the system's security characteristics. To guarantee the security and integrity of the encoded data, this could entail investigating

cutting-edge encryption algorithms or applying cutting-edge encryption strategies like homomorphic encryption. In order to serve a variety of application situations, the system will also be enhanced to enable the encoding of other media kinds, such as photographs and videos. The system will be rigorously tested and assessed in order to guarantee its efficacy. This approach will assess the system's resistance to potential attacks and compare its performance to that of other encoding schemes of a similar kind. This project's long-term objective is to solidify SC-ENC as a reliable and effective encoding solution, thereby satisfying the growing demand for secure data transfer and storage.

## REFERENCES

1. Babatunde, A. O., Dauda, S. O., Raji, A. K., Oladipo, I. D., Ogunwobi, Z. O., Taofeek-Ibrahim, F. A., & Balogun, G. B. (2023). A HYBRIDIZED ENCRYPTION SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY FOR SECURING DATA IN SMART HEALTHCARE. LAUTECH Journal of Engineering and Technology, 17(1), 45-64.
2. Syed, S. (2023). A New Generalized Signcryption Scheme Based on Elliptic Curves (Doctoral dissertation, CAPITAL UNIVERSITY).
3. Hadi, H. H., & Neamah, A. A. (2023). Diffie-hellman key exchange based on block matrices combined with elliptic curves. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 353-360.
4. Pandey, K., & Sharma, D. (2023, June). Advances in data security through elliptical curve cryptography. In AIP Conference Proceedings (Vol. 2819, No. 1). AIP Publishing.
5. Saeidi, M. R., & Mala, H. (2023). Secure Outsourcing of Two Standard Identity-Based Cryptosystems. ISeCure, 15(2).
6. Vishnubhai, P. K., & Shah, M. V. Design and Implementation of Efficient Elliptic Curve Cryptography on Reconfigurable Platforms.
7. De Smet, R., Blancquaert, R., Godden, T., Steenhaut, K., & Braeken, A. (2024). Armed with Faster Crypto: Optimizing Elliptic Curve Cryptography for ARM Processors. Sensors, 24(3), 1030.
8. Pande, D., Rawat, A. S., Deshmukh, M., & Singh, M. (2023). Single secret sharing scheme using chinese remainder theorem, modified Shamir’s scheme and XOR operation. Wireless Personal Communications, 130(2), 957-985.
9. Sanon, S. P., Alzalam, I., & Schotten, H. D. Quantum and Post-Quantum Security in Future Networks.
10. Salem, F. M., Safwat, M., Fathy, R., & Habashy, S. (2023). AMAKAS: Anonymous Mutual Authentication and Key Agreement Scheme for securing multi-server environments. Journal of Cloud Computing, 12(1), 128.
11. Elhajj, M., & Mulder, P. (2023). A comparative analysis of the computation cost and energy consumption of relevant curves of ecc presented in literature. International Journal of Electrical and Computer Engineering Research, 3(1), 1-6.
12. Komazawa, H., & Matsuzawa, T. (2023). Distributed attribute-based encryption with small ciphertext. Advances in the Theory of Nonlinear Analysis and its Application, 7(3), 30-44.
13. Zhang, Q., & Tian, Y. (2024). Cryptanalysis and improvement of “group public key encryption scheme supporting equality test without bilinear pairings”. Information Sciences, 120349.
14. Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. Cryptography, 7(3), 40.
15. Al-Amri, R. M., Hamood, D. N., & Farhan, A. K. (2023). Theoretical Background of Cryptography. Mesopotamian Journal of CyberSecurity, 2023, 7-15.