

Secure data encryption key scenario for protecting private data security and privacy

Sanjeev Kumar Mandal [§]

*Department of Computer Science and Engineering and Information Technology
Jain (Deemed to be University)
Bangalore
Karnataka
India*

Amit Sharma [†]

*Department of Computer Application
Lovely Professional University
Punjab
India*

Santosh Kumar Henge ^{*}

*Department of Computer Science & Engineering
Koneru Lakshmaiah Education Foundation
KL University
Andhra Pradesh
India*

Sumaira Bashir [‡]

Madhuresh Shukla [@]
*Department of Computer Application
Lovely Professional University
Punjab
India*

Asim Tara Pathak [#]

*Department of MDR Threat Analysis
MDR
Bangalore
India*

[§] E-mail: sanjeev.mandal93@gmail.com, km.sanjeev@jainuniversity.ac.in

[†] E-mail: amit.25076@lpu.co.in

^{*} E-mail: hingesanthosh@gmail.com (Corresponding Author)

[‡] E-mail: Sumaira13579@gmail.com

[@] E-mail: madhureshshukla88@gmail.com

[#] E-mail: asimindia2019@gmail.com

Abstract

Cryptography, specifically encryption, plays a pivotal role in protecting data from unauthorized access. However, not all encryption methods are equally effective, as some exhibit vulnerabilities. This research proposing a novel encryption method that builds upon established techniques to enhance data security. The proposed method combines the strengths of the Festial encryption method and the Advanced Encryption Standard (AES) to create an algorithm that exhibits superior resistance against attacks. The proposed encryption method successfully mitigates vulnerabilities, demonstrating enhanced resilience against unauthorized access attempts and minimizing the potential for data leakage. By prioritizing security and advancing encryption technologies, it can effectively protect personal information, maintain data confidentiality and integrity, and establish a safer digital environment for individuals and organizations.

Subject Classification: Primary 68M25, Secondary 68P25, 68P27.

Keywords: Cyber threats (CA), Advanced encryption standard (AES), Personal information (PI), Proactive measures (PAM), Sensitive information (SI), Internet of Things (IoT).

1. Introduction

Encryption involves the process of transforming plaintext information into a ciphered form that can only be deciphered with the appropriate decryption key [1-2]. By simulating real-world attack scenarios, which can assess the effectiveness of our encryption method and its ability to withstand sophisticated intrusion attempts. This research piece has the following goals: Section 1 comprises the introduction and investigate goal; Section 2 presents the related work that expresses the contextual information to the study related to encryption key implications and techniques to secure personal and private data; Section 3 includes the suggested methodology of secure data encryption key scenarios with key instances for protecting private data security and privacy; Section 4 includes the investigational outcomes; and Section 5 has incorporated the inference.

2. Related Work

Cyber attackers are using increasingly sophisticated techniques to penetrate systems, steal sensitive data, and disrupt operations. According to the author [5], many data security and encryption methods that are now in use have been rigorously examined, and their workflows have been graphically displayed [6][11-13]. The environment for network parallel computing is abstractly analyzed by author [7-10].

A classification of MEC entities was provided by author [12-15] and applied to specify protection restrictions based on Zero-Trust Security methodology. For hybrid cloud Internet of Things, author [16] suggests a multilayered, safe privacy protection solution built on Generative Adversarial Networks. Author [21] recommends the SP-MAACS scheme, a multi-authority access control system for cloud-based healthcare data sharing that is secure and protects privacy. A new ABE scheme created by author [28] safeguards user privacy when issuing keys [30]. [31–33]. The cloud server requires help from a Trusted Third Party (TTP) in order to communicate data because it has privacy issues with personal data [34] [37].

3. Methodology

The research findings demonstrate that the proposed encryption method successfully mitigates the vulnerabilities present in previous encryption techniques. It exhibits a higher level of resilience against brute force attacks, effectively thwarting unauthorized access attempts. Furthermore, our method demonstrates improved resistance to timing channel attacks, effectively minimizing the potential for data leakage during the encryption process.

The proposed method, depicted in Figure 1, aims to enhance encryption effectiveness, and overcome its vulnerabilities. Through the implementation of this improved encryption mechanism, the goal is to strengthen the protection of confidential information and ensure the integrity of data transmission and storage.

1st Round of encryption $K_i \oplus P_i = \text{ciphertext } 1$

2nd Key generation formula: $K_i < 3$ (only used once in Round 1)

It has used the Dcode tool to XOR the plaintext with the key, Figure 2 (a) and (b) shows the encryption of $K_i \oplus P_i$.

After 1st round of encryption

Ciphertext1: 00011011 00000100 00000010 00000110 00001010

Key 2: khood

The result will be transferred for the further process.

2nd round

2nd Round of encryption $K_i \oplus P_i = \text{ciphertext } 2$

2nd Key generation formula: K_i

Key 2: 01101011 01101000 01101111 01101111 01110010

Ciphertext 1: 00011011 00000100 00000010 00000110 00001010

After 2nd round of encryption as shown in Figure 3 (a)

Ciphertext 2: 01101011 01101000 01101111 01101111 01110010

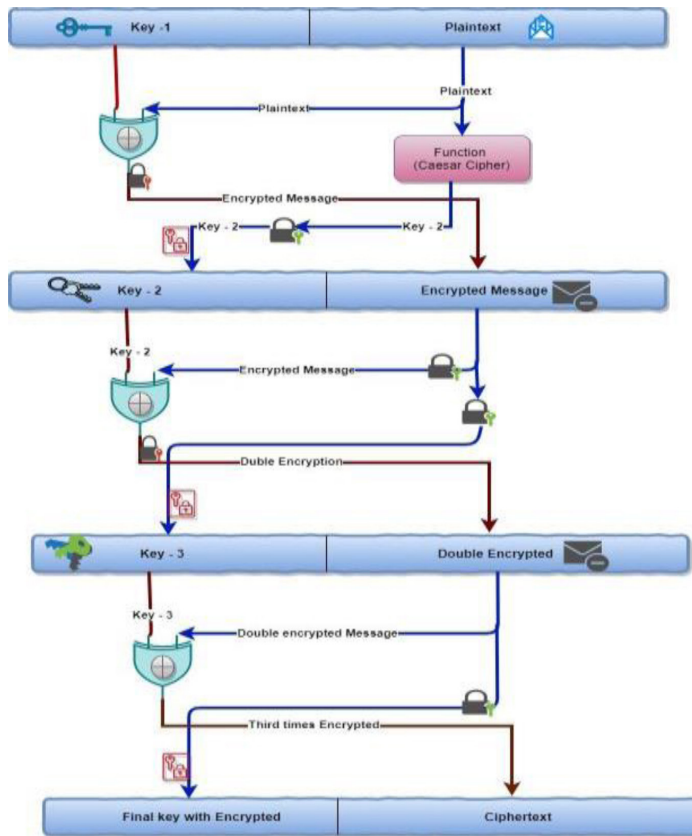


Figure 1

Secure Data Encryption Key Scenario for Protecting Private Data Security and Privacy



Figure 2

Integrated SPI and SPD with sample plaintext and primary stage of key

3rd round
Key 3: 00011011 00000100 00000010 00000110 00001010
Ciphertext 2: 01101011 01101000 01101111 01101111 01110010
After 3rd round of encryption
Ciphertext 3: 01101011 01101000 01101111 01101111 01110010
4th round
Key 4: 01110000 01101100 01101101 01101001 01111000
Ciphertext 3: 01101011 01101000 01101111 01101111 01110010



Figure 3

(a) Encryption process for round 1 (b) Encryption process for round 2



Figure 4

(a) Encryption process for round 3 (b) Encryption process for round 4

After 4th round of encryption as shown in Figure 3 (b)

Final Ciphertext: 00011011 00000100 00000010 00000110 00001010

Decryption

The proposed method utilizes a series of encryption rounds, where both the key and plaintext message are encrypted using the XoR function.

Final Key: 01110000 01101100 01101101 01101001 01111000

Final Ciphertext: 00011011 00000100 00000010 00000110 00001010

After performing the XOR function receiver needs to use Caesar cipher method to get a readable message. EX from the above description the ciphertext is: **khoor** this will be further decrypted with the help of Caesar cipher shift method $\gg 3$ to get the original message/plaintext as shown in Figure 4.

Khoor $\gg 3$ = hello (original plaintext)



Figure 5
Decryption process

4. Result and Discussion

To evaluate the security strength of the proposed method, the DCODE tool, a highly potent tool capable of analyzing and decrypting any ciphertext, was employed. The utilization of the comprehensive capabilities of the DCODE tool in this analysis lends credibility to the security robustness of the proposed method which integrated to analyze the brute-force attack with supporting access control rules and encryption key scenarios which has shown in Figure 2 to 4. The original data, encryption

level, instance of encryption, used key generation formula and generated cipher text along with key implications are shown in Table 1.

Table 1
The level of encryption instance, message, instance, key generation, generated cipher text and key implications

Level	Message Level	Instance of encryption	Key formula	Binary Text (cipher text)	Key Implication
1	Original Message	$K_i \oplus P_i =$ ciphertext 1	$K_i < 3$ (only used once in Round 1)	00011011 00000100 00000010 00000110 00001010	00011011 00000100 00000010 00000110 00001010
2	ciphertext 1	$K_i \oplus P_i =$ ciphertext 2	$K_i \oplus P_i =$ ciphertext 2	00011011 00000100 00000010 00000110 00001010	01101011 01101000 01101111 01101111 01110010
3	ciphertext 2	$K_i \oplus P_i =$ ciphertext 3	$K_i \oplus P_i =$ ciphertext 3	01101011 01101000 01101111 01101111 01110010	00011011 00000100 00000010 00000110 00001010
4	ciphertext 3	$K_i \oplus P_i =$ ciphertext 4	$K_i \oplus P_i =$ ciphertext 4	01101011 01101000 01101111 01101111 01110010	01110000 01101100 01101101 01101001 01111000
5	ciphertext 4	$K_i \oplus P_i =$ ciphertext 4 (final bit values)	$K_i \oplus P_i =$ ciphertext 4 (final bit values)	01110000 01101100 01101101 01101001 01111000	00011011 00000100 00000010 00000110 00001010

The comparative analysis and evaluation highlight the efficacy and advantages of the proposed encryption method. The Table 2 and Figure 5 is representing the qualified analysis of proposed methodology with existing methodologies based on various encryption type, strength and process of authentication and multi-authorization, access control, key size, and vulnerabilities (Vuls).

Table 2

Comparative exploration of intended methodology with active methodologies based on Authentication (Auth) and Multi-Authentication (MA) Process and key size

Encryption Method	Strength	Auth / MA Process	Key Size/Length in bits	Vulnerabilities (Vuls)
AES (Advanced Encryption Standard)	Very Strong	MA	128, 192, or 256 bits	No practical Vuls
RSA (Rivest-Shamir-Adleman)	Strong	MA	2048 bits or higher	weak keys
Blowfish	Moderate	MA	32-448 bits	partial weak keys
Two-fish	Strong	MA	128, 192, or 256 bits	No known practical Vuls
ChaCha20	Strong	MA	256 bits	No known practical Vuls
MD5 (Message Digest Algorithm 5)	Weak	MA	128 bits	Vuls to collision attacks
SHA-256 (Secure Hash Algorithm 256-bit)	Strong	MA	256 bits	No known practical Vuls
Proposed method	Strong	Dual Hybrid MA	128, 192, or 256 bits	No practical Vuls

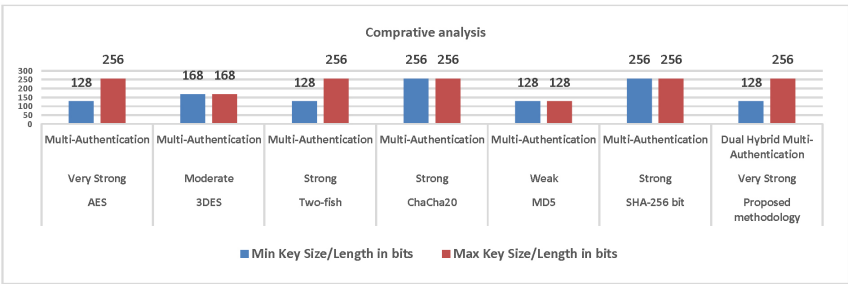


Figure 6

Comparative analysis of proposed methodology with existing methodologies

5. Conclusion

The proposed encryption method successfully mitigates vulnerabilities, demonstrating enhanced resilience against unauthorized access attempts and minimizing the potential for data leakage. By prioritizing security and advancing encryption technologies, it can effectively protect personal information, maintain data confidentiality and integrity, and establish a safer digital environment for individuals and organizations.

References

[1] H.-S. Wang, Z.-Y. Xu, Y. Zhang, K.-Y. Chen, B.-C. Li, and L.-A. Wu, "Attack on the advanced encryption standard cipher chip based on the correspondence between Hamming weight and the number of emitted photons," Wuli Xuebao/Acta Phys. Sin. (2016), doi: 10.7498/aps.65.118901.

[2] G. Lasry, M. Rubin, N. Kopal, and A. Wacker, "Cryptanalysis of Chaocipher and solution of Exhibit 6," Cryptologia (2016), doi: 10.1080/01611194.2015.1091797.

[3] R. Bhushan, B. Acharya, and A. Dwivedi, "A novel data place encryption algorithm," (2014), doi: 10.1109/ICDCCom.2014.7024691.

[4] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathemati-*

- cal Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.
- [5] Qureshi, M.B.; Qureshi, M.S.; Tahir, S.; Anwar, A.; Hussain, S.; Uddin, M.; Chen, C.-L. Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud. *Symmetry* 14, 695 (2022). <https://doi.org/10.3390/sym14040695>.
 - [6] Dhiman, P.; Henge, S.K.; Ramalingam, R.; Dumka, A.; Singh, R.; Gehlot, A.; Rashid, M.; Alshamrani, S.S.; AlGhamdi, A.S.; Alshehri, A. Secure Token–Key Implications in an Enterprise Multi-Tenancy Environment Using BGV–EHC Hybrid Homomorphic Encryption. *Electronics*, 11, 1942 (2022). <https://doi.org/10.3390/electronics11131942>.
 - [7] Leng Wang, Li Yang, “Constructing a Security System for Classified Computer Information Using Distributed Parallel Computing”, *Mobile Information Systems*, vol. 2022, Article ID 1195137, 12 pages (2022). <https://doi.org/10.1155/2022/1195137>.
 - [8] Zhu, X.; Srivastava, G.; M. Parizi, R. An Efficient Encryption Algorithm for the Security of Sensitive Private Information in Cyber-Physical Systems. *Electronics* 2019, 8, 1220. <https://doi.org/10.3390/electronics8111220>
 - [9] Ling Sun, Dali Gao, “Security Attitude Prediction Model of Secret-Related Computer Information System Based on Distributed Parallel Computing Programming”, *Mathematical Problems in Engineering*, vol. 2022, Article ID 3141568, 13 pages (2022). <https://doi.org/10.1155/2022/3141568>.
 - [10] Zhou, Y.; Zheng, S.; Wang, L. Privacy-Preserving and Efficient Public Key Encryption with Keyword Search Based on CP-ABE in Cloud. *Cryptography*, 4, 28 (2020). <https://doi.org/10.3390/cryptography4040028>.
 - [11] M. Ali, C. Xu and A. Hussain, “Authorized attribute-based encryption multi-keywords search with policy updating,” *Journal of New Media*, vol. 2, no.1, pp. 31–43 (2020). <https://doi.org/10.32604/jnm.2020.09946>.
 - [12] Lee, J.; Kim, M.; Oh, J.; Park, Y.; Park, K.; Noh, S. A Secure Key Aggregate Searchable Encryption with Multi Delegation in Cloud Data

- Sharing Service. *Appl. Sci.* 11, 8841 (2021). <https://doi.org/10.3390/app11198841>.
- [13] P. Dhiman, S. K. Henge, S. Singh, A. Kaur, P. Singh et al., "Blockchain merkle-tree ethereum approach in enterprise multitenant cloud environment," *Computers, Materials & Continua*, vol. 74, no.2, pp. 3297–3313 (2023), <https://doi.org/10.32604/cmc.2023.030558>.
- [14] Belal Ali, Simsam Hijjawi, Leith H. Campbell, Mark A. Gregory, Shuo Li, "A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing", *Security and Communication Networks*, vol. 2022, Article ID 3178760, 14 pages (2022). <https://doi.org/10.1155/2022/3178760>.
- [15] Adee, R.; Mouratidis, H. A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*, 22, 1109 (2022). <https://doi.org/10.3390/s22031109>.
- [16] Budati, A.K.; Vulapula, S.R.; Shah, S.B.H.; Al-Tirawi, A.; Carie, A. Secure Multi-Level Privacy-Protection Scheme for Securing Private Data over 5G-Enabled Hybrid Cloud IoT Networks. *Electronics*, 12, 1638 (2023). <https://doi.org/10.3390/electronics12071638>.
- [17] Henge, S.K.; Maheswari, G.U.; Ramalingam, R.; Alshamrani, S.S.; Rashid, M.; Murugan, J. Dependable and Non-Dependable Multi-Authentication Access Constraints to Regulate Third-Party Libraries and Plug-Ins across Platforms. *Systems*, 11, 262 (2023). <https://doi.org/10.3390/systems11050262>.
- [18] Gupta, A. K. Singh, C. -N. Lee and R. Buyya, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions," in *IEEE Access*, vol. 10, pp. 71247-71277 (2022), doi: 10.1109/ACCESS.2022.3188110.
- [19] Alsulbi, K.A.; Khemakhem, M.A.; Basuhail, A.A.; Eassa, F.E.; Jambbi, K.M.; Almarhabi, K.A. A Proposed Framework for Secure Data Storage in a Big Data Environment Based on Blockchain and Mobile Agent. *Symmetry* 2021, 13 (1990). <https://doi.org/10.3390/sym13111990>.
- [20] Santosh Kumar Henge, Gitanjali Jayaraman, M Sreedevi, R Rajakumar, Mamoon Rashid, Sultan S. Alshamrani, Mrim M. Alnfiai, Ahmed Saeed AlGhamdi. Secure keys data distribution based user-storage-transit server authentication process model using mathemat-

- ical post-quantum cryptography methodology[J]. *Networks and Heterogeneous Media*, 18(3): 1313-1334 (2023). doi: 10.3934/nhm.2023057.
- [21] Gupta, R.; Kanungo, P.; Dagdee, N.; Madhu, G.; Sahoo, K.S.; Jhanjhi, N.Z.; Masud, M.; Almalki, N.S.; AlZain, M.A. Secured and Privacy-Preserving Multi-Authority Access Control System for Cloud-Based Healthcare Data Sharing. *Sensors*, 23, 2617 (2023). <https://doi.org/10.3390/s23052617>.
- [22] Luo, W.; Ma, W. Secure and Efficient Data Sharing Scheme Based on Certificateless Hybrid Signcryption for Cloud Storage. *Electronics*, 8, 590 (2019). <https://doi.org/10.3390/electronics8050590>.
- [23] Henge, S.K., Rama, B., Five-Layered Neural Fuzzy Closed-Loop Hybrid Control System with Compound Bayesian Decision-Making Process for Classification Cum Identification of Mixed Connective Consonants and Numerals. *Advances in Intelligent Systems and Computing*, vol 553. Springer, Singapore (2017). https://doi.org/10.1007/978-981-10-3770-2_58.
- [24] Radi P. Romansky, Irina S. Noninska. Challenges of the digital age for privacy and personal data protection[J]. *Mathematical Biosciences and Engineering*, 17(5): 5288-5303 (2020). doi: 10.3934/mbe.2020286.
- [25] Singh, B., Henge, S.K., Neural Fuzzy Inference Hybrid System with Support Vector Machine for Identification of False Singling in Stock Market Prediction for Profit Estimation. *INFUS 2020. Advances in Intelligent Systems and Computing*, vol 1197. Springer (2021), Cham. https://doi.org/10.1007/978-3-030-51156-2_27.
- [26] S. K. Henge and B. Rama, "Neural fuzzy closed loop hybrid system for classification, identification of mixed connective consonants and symbols with layered methodology," *IEEE ICPEICES*, pp. 1-6 (2016), doi: 10.1109/ICPEICES.2016.7853708.
- [27] Zhang, D.; Chen, J.; He, Y.; Lan, X.; Chen, X.; Dong, C.; Li, J. A Chunked and Disordered Data Privacy Protection Algorithm: Application to Resource Platform Systems. *Appl. Sci.*, 13, 6017 (2023). <https://doi.org/10.3390/app13106017>.
- [28] Yujiao Song, Hao Wang, Xiaochao Wei, Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud", *Security and Com-*

- munication Networks, vol. 2019, 9 pages (2019). <https://doi.org/10.1155/2019/3249726>.
- [29] Yang Yu, "Encryption Technology for Computer Network Data Security Protection", Security and Communication Networks, vol. 2022, Article ID 1789222, 9 pages (2022). <https://doi.org/10.1155/2022/1789222>.
- [30] AlShalaan, M.R.; Fati, S.M. Enhancing Organizational Data Security on Employee-Connected Devices Using BYOD Policy. Information, 14, 275 (2023). <https://doi.org/10.3390/info14050275>.
- [31] Henge, Santosh Kumar, Upadhyay, Aditya, Saini, Ashok Kumar, Mishra, Neha, Sharma, Dimpal & Sharma, Gajanand. Analysis and detection of insider attacks using behaviour rule based architecture in enterprise multitenancy, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 707-718 (2023), DOI: 10.47974/JD-MS-1743.