Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 2005–2014
DOI : 10.47974/JDMSC-2362

Multilayer encryption cipher mitigating salting sequence key approach for securing transit data

Sanjeev Kumar Mandal [@]
Ravleen Singh [†]
N. Chandu [§]
Department of Computer Science & Information Technology
Jain (Deemed-to-be University)
Bangalore
Karnataka
India

M. Padmavathi [‡]
Department of Computer Science & Engineering
Swarna Bharathi Institute of Science and Technology (SBIT)
Khammam
Telangana
India

Santosh Kumar Henge *
Chanakya Kumar Hinge [#]
Department of Computer Science and Engineering
School of Computer Science and Artificial Intelligence
SR University
Warangal 506371
Telangana
India

[@] *E-mail:* sanjeev.mandal93@gmail.com
[†] *E-mail:* ravleen1234@gmail.com
[§] *E-mail:* chandunagesh2302@gmail.com
[‡] *E-mail:* macherlapadmavathi@gmail.com
* *E-mail:* hingesanthosh@gmail.com (Corresponding Author)
[#] *E-mail:* hingechanakya7@gmail.com

© Taru Publications

Venkateswarlu Sunkari [$]
Department of Artificial Intelligence & Data Science
Koneru Lakshmaiah Education Foundation
Vaddeswaram 520002
Andhra Pradesh
India

Amit Sharma [^]
Department of Computer Application
School of Computer Application
Lovely Professional University
Jalandhar 144402
Punjab
India

Abstract

In order to secure data through broadcast in excess of set of connections, secure data accumulated on cloud proposals and mobile devices, enable protected message during certificate authority (CT) based trusted third party environment (TTPE), and guarantee data integrity. These security issues can be successfully overcome with the help of this research, which suggests a multilayer encryption cipher (MLEC) mitigation salting sequence key technique for protected transportation data. The investigational scenario defined with three layers is the MLEC mitigation salting sequence key strategy for safeguarding transit (PT) data. First layer integrated the encryption process using ASCII-based ciphering to convert plaintext to ASCII-HEX code. The layer-2 (L2) integrated the encryption process using XOR and key to produce encrypted HEX code and the third layer linked the salting sequences technique with key implications. The best success rate was obtained by designing and testing the experimental test cases in an enterprise cluster environment. Extenuating salting with MLEC provides secure transportation data devoid of any hacking.

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

Keywords: *Certificate authority (CT), Trusted third party environment (TTPE), Secure sockets layer (SSL), Secure sockets layer (TLS), Multilayer encryption cipher (MLEC).*

1. Introduction

In our digitally associated civilization, information security has happen to more and more challenging due to dangers variety from cyber attacks to unconstitutional admittance [1]. In this digitally connected

[$] *E-mail:* **sunkarivenkateswarlu@kluniversity.in**
[^] *E-mail:* **amit.25076@lpu.co.in**

society, the demands on information security are growing. However, encryption has evolved into a potent appliance for resolving these issues [2-4]. By encrypting data transmitted among clients and web-servers, cryptographic protocols [5] like Secure Sockets Layer (SSL) have addressed this risk and ensured confidentiality and integrity [6-8]. Secure communication is made possible by certificate authority (CT) based trusted third party environment (TTPE) [9-12], which permits the swap over of keys encryption which verifies the identities of parties concerned. Hashing techniques in cryptography are also employed to secure password storage and guarantee data integrity [13-17]. Therefore, our algorithm's multilayer technique will aid in resolving this problem.

This research organized as follows: The relevant work, which articulates the study's context, is presented in section 2. The suggested three-layer multilayer (ML) encryption cipher (MLEC) mitigation salting technique for protecting transit data is included in Section 3 along with the consequences of ASCII-based ciphering by layer 1 (L1). Included results and discussion are Section 4, and the conclusions and future directions are articulated in Section 5.

2. Related Work

This paper's base is security, wherein a range of symmetric algorithmic approaches such as classical and current cryptography, and so forth—are investigated. We developed the idea of cipher-ASCII with ML approach because the greater part of these algorithmic sequences lacked well-built encryption techniques [10].

Homomorphic encryption is the most modern and safe way to protect data on cloud server [18][19] which permits computational procedures on encrypted data because it does not require the data to be decrypted in order to be development [22-25]. A symmetric key approach was recommended by another study for both encryption and decryption [26-29]. A proposed method that makes the process safer by combining the replacement methodology, ASCII codes, and the XOR operation [30–33].

3. Methodology

This approach combined multiple layers of cipher encryption to analyze and monitor different cyber attacks, threads, and malware on transportation data that is in transit method from end user to peers. The suggested methodology used blended layers that synced with two levels:

the Mitigating Salting Sequence (MSS) and the ciphering ASCII were supplied in L2 as shown in Figure 1.

3.1 *Layer 1 Encryption: Plaintext-ASCII-HEX Code via ASCII-based Ciphering*

First, the PT communication is transformed into ASCII characters via the stage 1 encryption. Next, every ASCII quality is translated into its matching HEX code which then encrypted with an XOR with key. The term "XOR" describes a particular type of logic gate that this sequences uses to perform the restricted OR operation [13]. The encryption and decryption processes had both involved the key that is symbolize by the HEX color code keys. The hex codes are created using the color theory [20] formula, where R stands for red, G for green, and B for blue.

3.2 *Key with XOR Implications for Encrypted Hex Code (EHC) in Layer 2 Encryption*

Each code HEX is encrypted with keys in this section. Let's XOR the corresponding key with each code HEX with the following HEX-EHC color code key represents a keys like as: #FF0000, #000000, and #00FF00.

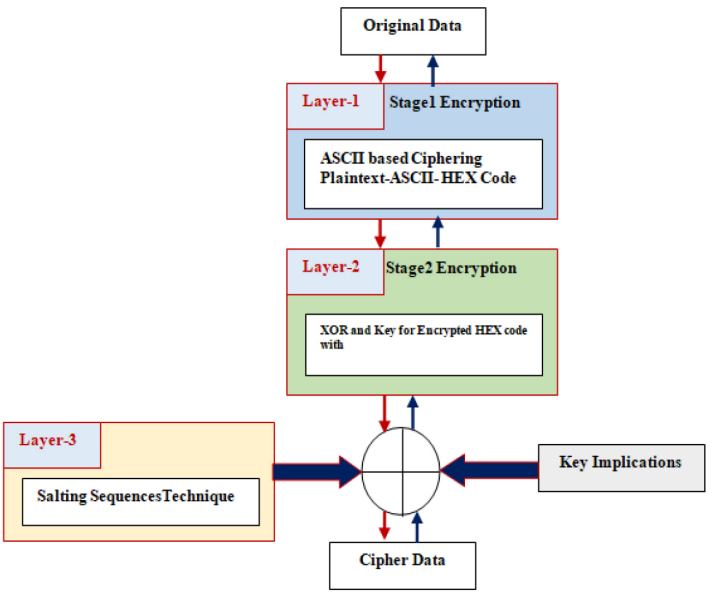

Figure 1

Geometric identical and multilayer encryption cipher (MLEC) environment

3.2.1 HEX Code to Twofold Conversion

The binary values are 01001000 = 48 (HEX) = 00 (HEX) = 00000000. Apply the XOR function to every join up of matching bits: The concluding twofold bits of XOR for 48 † 01001000 and 00 † 00000000 => 01001000 are referenced. 01001000(Binary) = 48(HEX) is the result of converting the twofold results back to HEX.

3.3 *Layer 3 Encryption: The Method of Mitigating Salting Sequence (MSS)*

The sequence of salting (SS) appearance in cryptography submits to the addition of arbitrary statistics to a hash purpose input in order to guarantee a exclusive outcomes yet in cases where inputs are equal [21].

3.4 *Cipher Text (CT) Decryption*

In the process of decrypting CT processed with a single key, every encrypted color HEX code is decrypted with XOR; here every decrypted code HEX is then converted reverse hooked on its ASCII illustration; original plaintext message is then obtained by concatenating the ASCII characters. The provided CT is protected next to occurrence investigation and brute force attacks by the decode tool's output.

4. Result and Discussion

To secure the data and key, several authentication procedures are used in conjunction with multiple encryption processes. As seen in Table 1, the first level of encryption was implemented by translating plaintext to ASCII and then HEX Code references.

Table 1

Encryption Mapping of RKI 1 through 3 and the final outcome of the sequences inference

RKI-1 with XOR	RKI-2 with XOR	RKI-3	Final RKI
48	00000000	01001000	48
45	00000000	01000101	45
4C	00000000	01001100	4C
FF	11111111	10110011	B3
4F	00000000	01001111	4F

Table 2

Sequence-inferred final output and mapping of DRKI from 1 to 3

DRKI-1 with XOR	DRKI-2 with XOR	DRKI-3	Final DRKI
48	00000000	01001000	(48)
45	01000101	01000101	((48)(45))
4C	00000000	01001100	((48)(45)(4C))
FF	00000000	01001100	((48)(45)(4C)(45))
B3	11111111	01001100	(((48) (4C)) ((45)(4C)))
4F	00000000	01001111	(((48) (4C)) ((45)(4C)) (4F))

4.1 *Layer of Multi-Encryption Process*

For 48 † 01001000; 00 † 00000000 => 01001000, the PT-ASCII-HEX Code is referred to as a final XOR binary bits in layer 1. 01001000(Binary) = 48(HEX) is the result of converting the twofold consequences back to HEX.

4.2 *Layer of the Decryption Process*

Table 2 displays the final output of decryption, which is the mapping of DRKI through 1 to 3.

Table 2 displays the final output of the HEX conversion and mapping, decryption primary, 2nd major, sub-progression of DPS from 1 to 2, DSS from 1 to 2, replication keys, and succession inference.

5. Conclusion

The investigational development defined through three layers is the MLEC mitigation salting progression key strategy for safeguarding transit data. The first layer integrated the encryption process, processing stage 1 using ASCII-based ciphering to convert PT to ASCII-HEX code; the second layer included the encryption process, processing stage 2 using XOR with key to produce encrypted code HEX; and the L-3 linked the salting sequences technique with key implications.

References

[1] C. Rupa, Greeshmanth, and M. A. Shah, "Novel secure data protection scheme using Martino homomorphic encryption," *J. Cloud Comput.*, vol. 12, no. 1 (2023), doi: 10.1186/s13677-023-00425-7.

[2] K. Begovic, A. Al-Ali, and Q. Malluhi, "Cryptographic ransomware encryption detection: Survey," *Comput. Secur.,* vol. 132 (2023), doi: 10.1016/j.cose.2023.103349.

[3] V. Sivagaminathan, M. Sharma, and S. K. Henge, "Intrusion detection systems for wireless sensor networks using computational intelligence techniques," *Cybersecurity*, vol. 6, no. 1, p. 27 (2023), doi: 10.1186/s42400-023-00161-0.

[4] R. M. Al-Amri, D. N. Hamood, and A. K. Farhan, "Theoretical Background of Cryptography," *Mesopotamian Journal of CyberSecurity*, vol. 2023 (2023). doi: 10.58496/MJCS/2023/002.

[5] I. V. Martynenkov, "The main stages of development of the cryptographic protocols SSL/TLS and IPsec," *Prikl. Diskretn. Mat.*, no. 51 (2021), doi: 10.17223/20710410/51/2.

[6] K. Y. Chai and M. F. Zolkipli, "Review on Confidentiality, Integrity and Availability in Information Security," *J. ICT Educ.*, vol. 8, no. 2 (2021), doi: 10.37134/jictie.vol8.2.4.2021.

[7] A. J. S. Bhargav and A. Manhar, "A Review on Cryptography in Cloud Computing," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol*. (2020), doi: 10.32628/cseit206639.

[8] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," *Int. J. Comput. Sci. Mob. Comput.,* vol. 13, no. 1 (2024), doi: 10.47760/ijcsmc.2024.v13i01.007.

[9] D. Kent, B. H. C. Cheng, and J. Siegel, "Assuring Vehicle Update Integrity Using Asymmetric Public Key Infrastructure (PKI) and Public Key Cryptography (PKC)," *SAE Int. J. Transp. Cybersecurity Priv.,* vol. 2, no. 2 (2020), doi: 10.4271/11-02-02-0013.

[10] F. D. T. Amijaya, S. Syaripuddin, Q. Q. A'yun, Y. N. Nasution, W. Wasono, and M. N. Huda, "Hill cipher algorithm using two keywords and 94 ASCII characters," in AIP Conference Proceedings (2022). doi: 10.1063/5.0111696.

[11] N. Sharma and P. Mca Scholar, "A Review of Information Security using Cryptography Technique," *Int. J. Adv. Res. Comput. Sci.,* vol. 8, no. 4 (2017).

[12] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *Int. J. Adv. Comput. Sci. Appl.,* vol. 9, no. 3 (2018), doi: 10.14569/IJACSA.2018.090354.

[13] A. Bernasconi, S. Cimato, V. Ciriani, and M. C. Molteni, "Multiplicative Complexity of XOR Based Regular Functions," I*EEE Trans. Comput.*, vol. 71, no. 11 (2022), doi: 10.1109/TC.2022.3141249.

[14] M. Abdulla, "Vulnerabilities in Public Key Cryptography," *Int. J. Psychosoc. Rehabil.*, vol. 24, no. 5 (2020), doi: 10.37200/ijpr/v24i5/pr202096.

[15] Fina Triana, Jon Endri, and Irma Salamah, "Implementation of CAESAR CIPHER Cryptography Techniques for Android Based Information Data Security," *J. RESTI* (Rekayasa Sist. dan Teknol. Informasi), vol. 4, no. 4 (2020), doi: 10.29207/resti.v4i4.1984.

[16] A. Patil, S. Mulik, P. Pathak, and K. Raut, "Review paper on Data Security using Cryptography and Steganography," (2021).

[17] D. G. S. P. H. Biradar, "Avoidance of Unauthorized user using Visual Cryptography," *Int. J. Sci. Res.*, vol. 5, no. 8 (2016).

[18] V. Kumar, S. Ray, M. Dasgupta, and M. K. Khan, "A Pairing Free Identity Based Two Party Authenticated Key Agreement Protocol Using Hexadecimal Extended ASCII Elliptic Curve Cryptography," *Wirel. Pers. Commun.*, vol. 118, no. 4 (2021), doi: 10.1007/s11277-021-08168-x.

[19] J. R. Paragas, A. M. Sison, and R. P. Medina, "An Improved Hill Cipher Algorithm using CBC and Hexadecimal S-Box," in 2019 IEEE Eurasia Conference on IOT, Communication and Engineering, ECICE 2019 (2019). doi: 10.1109/ECICE47484.2019.8942717.

[20] Panchami Vijayan, "A NEW COLOR ORIENTED CRYPTOGRAPHIC ALGORITHM BASED ON UNICODE AND RGB COLOR MODEL," *Int. J. Res. Eng. Technol.*, vol. 03, no. 13 (2014), doi: 10.15623/ijret.2014.0313016.

[21] Dan Arias, Adding Salt to Hashing: A Better Way to Store Passwords, https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/ (Accessed on 24th June-2024).

[22] P. Dhiman and S. K. Henge, "Analysis of blockchain secure models and approaches based on various services in multitenant environment," in Recent Innovations in Computing, Lecture Notes in Electrical Engineering, vol. 855, Springer, Singapore (2022), doi: 10.1007/978-981-16-8892-8_42.

[23] D.-E.-S. Agha, S. A. Khan, H. Fakhruddin, and H. H. Rizvi, "Security enhancing by using ASCII values and substitution technique for

symmetric key cryptography," *Indian Journal of Science and Technology*, vol. 10, no. 36 (Sep. 2017), doi: 10.17485/ijst/2017/v10i36/119181.

[24] P. Dhiman and S. K. Henge, "Comparative analysis of cloud security complexities and past proposed nonhomomorphic and homomorphic encryption methodologies with limitations," in ICT for Competitive Strategies, vol. 1, CRC Press, pp. 787–799 (2020), doi: 10.1201/9781003052098-83.

[25] V. Sivagaminathan, M. Sharma, and S. K. Henge, "Integration of deep neural network architecture for network intrusion detection system," in Recent Advances in Computing Sciences, CRC Press, pp. 1–6 (2023).

[26] K. Loyka, H. Zhou, and S. P. Khatri, "A homomorphic encryption scheme based on affine transforms," in Proc. 2018 Great Lakes Symp. VLSI (GLSVLSI '18), New York, NY, USA: ACM, pp. 51–56 (2018), doi: 10.1145/3194554.3194585.

[27] S. K. Henge, A. Upadhyay, A. K. Saini, N. Mishra, D. Sharma, and G. Sharma, "Analysis and detection of insider attacks using behaviour rule based architecture in enterprise multitenancy," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 3, pp. 707–718 (2023), doi: 10.47974/JDMSC-1743.

[28] A. Upadhyay, R. Misra, S. K. Henge, and Y. Bhardwaj, "Protection of digital image and text information security using LSB and crossover techniques," in Computational Vision and Bio-Inspired Computing, S. Smys, J. M. R. S. Tavares, and F. Shi, Eds., Advances in Intelligent Systems and Computing, vol. 1439, Springer, Singapore (2023), doi: 10.1007/978-981-19-9819-5_43.

[29] S. K. Henge, G. U. Maheswari, R. Ramalingam, S. S. Alshamrani, M. Rashid, and J. Murugan, "Dependable and non-dependable multi-authentication access constraints to regulate third-party libraries and plug-ins across platforms," *Systems*, vol. 11, no. 5, p. 262 (2023), doi: 10.3390/systems11050262.

[30] H. A. Abdallah and S. Meshoul, "A multilayered audio signal encryption approach for secure voice communication," *Electronics*, vol. 12, no. 1, p. 2 (2023), doi: 10.3390/electronics12010002.

[31] A. A. Raj, A. Beno and R. Jaisakthi, "Security Enhancement of Information using Multilayered Cryptographic Algorithm," 2020 4th International Conference on Trends in Electronics and Informatics

(ICOEI)(48184), Tirunelveli, India, pp. 348-353 (2020), doi: 10.1109/ICOEI48184.2020.9143052.

[32] Santosh Kumar Henge, Gitanjali Jayaraman, M. Sreedevi, R. Rajakumar, Mamoon Rashid, Sultan S. Alshamrani, Mrim M. Alnfiai, and Ahmed Saeed AlGhamdi, "Secure keys data distribution based user-storage-transit server authentication process model using mathematical postquantum cryptography methodology," *Networks and Heterogeneous Media,* vol. 18, no. 3, pp. 1313–1334 (2023), doi: 10.3934/nhm.2023057.

[33] Fauziyah, Zhaoshun Wang, Mujahid Tabassum, A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security, Computers, Materials & Continua, Vol. 78, no. 3, pp. 4417-4452 (2024), http://www.techscience.com/cmc/v78n3/55899.

Received November, 2024