JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

A HYBRID ENCRYPTION TECHNIQUE FOR DATA SECURITY IN SCM WITH IOT NETWORK

Dulal Kumbhakar[1*], Kanchan Sanyal[2] and Sunil Karforma[3]

[1*]Department of B.C.A., Vivekananda Mahavidyalaya, Hooghly, W. B., India

[2]Asst.Teacher, Computer Application, Bhadrapur M.N.K High School, Birbhum, W, B., India

[3]Department of Computer Science, The University of Burdwan, Bardhaman, West Bengal, India

[*]Corresponding Email: dulalkumbhakar69@gmail.com

ABSTRACT

Supply chain management (SCM) is the set of assigned elements required to manage, control and execute the flow of goods and services from raw materials to final products and also dissemination of finished products to a business's customers in efficiently with more economical way possible. Nowadays, many logistic companies adopt IoT network in connecting various devices used as a part of SCM to achieve the better operational efficiency of the SCM working flows. Hence, the various security vulnerabilities may arise due to the week data security mechanisms at the time of sharing collected sensitive data by IoT devices among the different levels of SCM or at the event of storing this data to the cloud and big data centers. For the purpose of the data security, we have proposed a novel chaos based hybrid encryption technique through Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) 256 bit Encryption algorithm in securing device authenticity as well as confidentiality of the services in IoT based SCM. In this work, firstly, Elliptic-curve Diffie-Hellman (ECDH) key exchange protocol is used to generate ECC key pair and then ECC secret key is XORed with the key generated by logistic map method to increase the randomness of the keys. After that ECC shared key is transformed into AES 256 bit secret key through MD5 hashing technique in encrypting the input files. Further, the execution time with throughput regarding encryption and description time is computed to measure the performance efficiency of the work. Again, entropy values of the encrypted files are also calculated to measure the security strength. Based on the experiment results, our proposed hybrid encryption technique through computation time with entropy measurement is more fast and secure compared to other existing techniques.

KEYWORDS: *Elliptic curve cryptography, ECDH, logistic map, AES, throughput and entropy.*

1. INTRODUCTION

SCM is a system of organizations, people, activities, information, and resources, which is involved in managing and controlling the several working flows like supply and demand, warehousing, inventory tracking, order entry, order management, distribution and delivery to the end customer. Nowadays, the business organizations are tried to expand the SCM working flows effectively and efficiently through IoT network in real time. The term, Internet of Things

Submitted: 17/10/2022 **Accepted**: 10/11/2022

(IoT), was first proposed by Kevin Ashton in 1999 [1], is a system of interconnected physical devices that are remotely monitored and controlled via internet and IoT is becoming a more popular mainstream in SCM working flows due to its endless capabilities with efficient numerous applications .Now, how to monitor and control the data or information from one level to another level of SCM based on IoT applications through internet is shown below the figure.

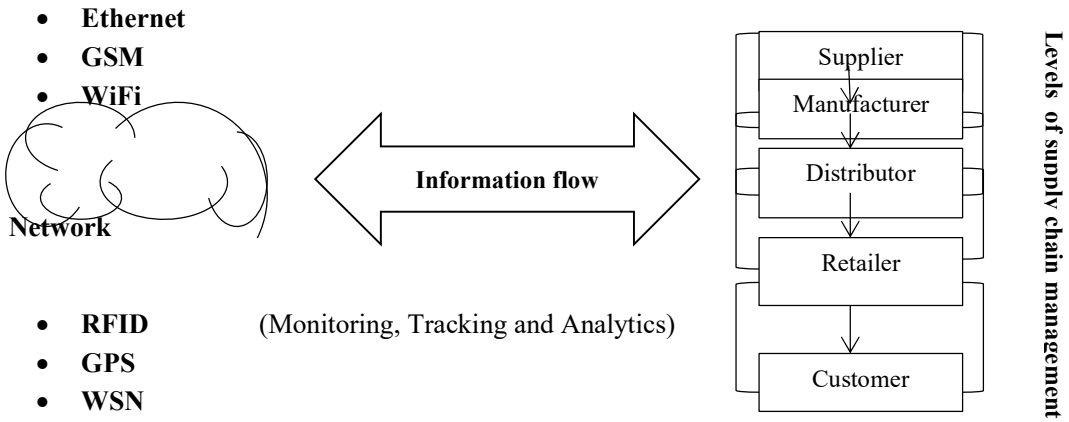


Fig-1: IoT based Supply Chain Management

According to Gartner, at least 50% of large scale global companies will be adopted the IoT based applications by 2023 for transforming the SCM both in terms of its operational efficiencies as well as revenue opportunities in making it more transparent [2]. IoT based supply chains not only tracking the product's information but also help to improve the quality of decision-making and predict the delivery as well as forecast in real time. Hence, from the manufacturer to the end customer in SCM by allowing IoT sensor devices (RFID, WSN, etc.) in the right way, IoT applications can make the SCM as professionals for all involved parties in SCM environment.

Regarding to the use of IoT in SCM, There are several security attacks like Denial of Service (Dos), replay attack, data leakage and other malicious activities from the cyber attackers can happen at any levels of SCM working flows. As a result, it can lead to a severe damaging situation to the integrity of the products or services, the privacy of their data, confidentiality of the services and the transactions in respect of organization's financial, operational, and brand consequences. In this context, the secure lightweight based security technique is required to encrypt the data which are generated or transmitted at the different working levels in SCM through IoT based resource constrained applications. In this regard, our Chaos based hybrid (ECC-AES) Encryption Technique is more suitable for resource-constrained applications or devices. The encryption will be performed at the any working phases of SCM which are connected through IoT applications before sending or uploading the data to the receiver end or

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

cloud server so that the data is not exposed by intruders. The intended recipients firstly decrypt the data and then examine the data in details as per requirements.

The paper is organized as follows: Section 2 represents the contributions of the work. Section 3 focuses the related works regarding data security in SCM with IoT network and section 4 proposes the chaos based hybrid encryption technique through ECC and AES 256 bit algorithm. Section 5 depicts the experiment results based on the performance efficiency as well as security strength with comparative analysis. Section 6 concludes the paper.

2. OUR CONTRIBUTIONS

Although many security mechanisms have been developed to secure data transmission in the IoT supply chain system, but many security vulnerabilities like Man in the Middle attack, brute force attacks and eavesdropping attacks are still active to severe the SCM working flows. Regarding security perspective, a new hybrid encryption technique through logistic map random number generation is proposed to protect the sensitive data of IoT based SCM system. The contributions of this work are: (a) Develop a secure and efficient data security system in IoT based SCM environment. (b) Improving the randomness of the secret key by chaos based logistic map. (c) Encrypting the text files through elliptic curve based key exchange protocol and AEC encryption technique in which key pair (public & private) generation and encryption are done by ECDH algorithm and 256 bit-AES algorithm respectively. (d) Increasing the device authenticity as well as the confidentiality of the services based on secrecy analysis. This work is also more suitable for resource constrained applications or devices used in IoT based SCM environment in which minimal computation time with consuming less memory is needed to implement or run such devices or applications in improving the security performance.

3. RELATED WORKS

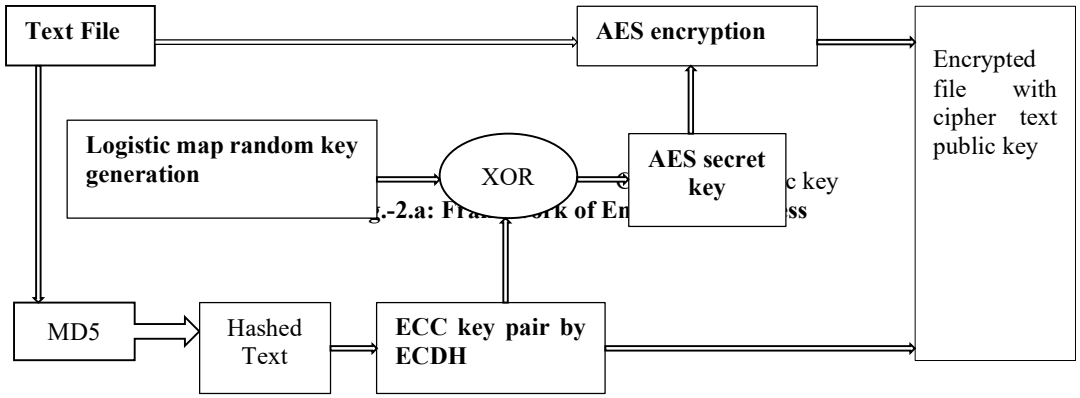
In this section, we have explained the several types of hybrid encryption mechanisms which are contributed on the security domain of IoT based applications by the many researchers. A. Ragab et al. [3] have proposed a hybrid encryption technique that combines ECC, XXTEA, SHA256, and Chaos random key generator in achieving the security requirements of cryptography including confidentiality, authenticity, integrity, and non-repudiation to protect IoT sensor devices from the attackers. They showed the experiment results based on execution time that the hybrid encryption through XXTEA with ECC technique is faster than the hybrid encryption technique based on XXTEA with RSA as well as proposed technique gives better throughput by 40%. S. K. Mousavi et al. [4] proposed a new hybrid security system based on Rivest cipher (RC4), Elliptic-Curve Cryptography (ECC), and Secure Hash Algorithm (SHA-256) to improve the data integrity of IoT-based smart irrigation systems. Based on the comprehensive analysis, they have indicated that this work is secured than other existing security techniques in protecting the sensitive information from the well-known attacks such as the Man-in-the-middle (MiM) attack. Also, the simulated results depict the effectiveness of the work based on encryption/decryption time, throughput, and security. Farooq and Zhu have analyzed supply chain risks in respect of IoT systems and they have suggested that the comprehensive risk assessment and impact analysis in achieving the concrete solutions

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

regarding the mitigation of supply chain risks in IoT systems [5]. S. Rehman et al. [6] have proposed a hybrid optimized security scheme by combining the ECC and AES technique to ensure authentication and data integrity requirements in securing the sharing data over the cloud. Based on experimental performance, they concluded that the proposed scheme is efficient compared with existing security mechanisms. Ming-Shen Jian et al. [7] have proposed a hybrid cryptosystem for securing the exchanged data among the IoT devices by combining the software defined network and Self-identification with Cryptosystem. Here, public key cryptosystem is used while exchanging the data from IoT device to server and vice versa. The experiment results shows the feasibility of the work which could help to improve the security performance of the connected IoT devices. S. Mukherjee et al. [8] proposed a hybrid security system in connection with RFID enabled Supply Chain Management system to secure the data transaction procedure through modified Wired Equivalent Encryption (WEP) and RSA cryptosystem. This proposed work is also addressed the short comings of WEP key algorithm so that it can be more secured compared to other existing related works by modified WEP encryption process. S. Rajesh et al. [9] have proposed a novel tiny symmetric encryption algorithm (NTSA) for improving the security while transferring the text files through the IoT network. It also produces more confusion on the key dynamically than tiny encryption algorithm for each round of encryption. M. Abu-Faraj and Z. Alqadi [25] have introduced a new Highly Secure Data Encryption (HSDE) technique to increase the data security level through a complex PK. The proposed technique is testified by several standard measurement metrics to measure the performance efficiency of the work.

4. PROPOSED HYBRID SECURITY SYSTEM

Our proposed hybrid security system is classified into three phases as EC curve based key generation through ECDH algorithm, pseudorandom number generation by logistic map, Encryption process and Decryption process through AES 256 bit technique. The ECC-AES with chaotic based data security framework of IoT supply chain management is shown in the following Fig.-2.a and Fig.-2.b respectively.



g.-2.a: Fra[illegible]rk of En[illegible]

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

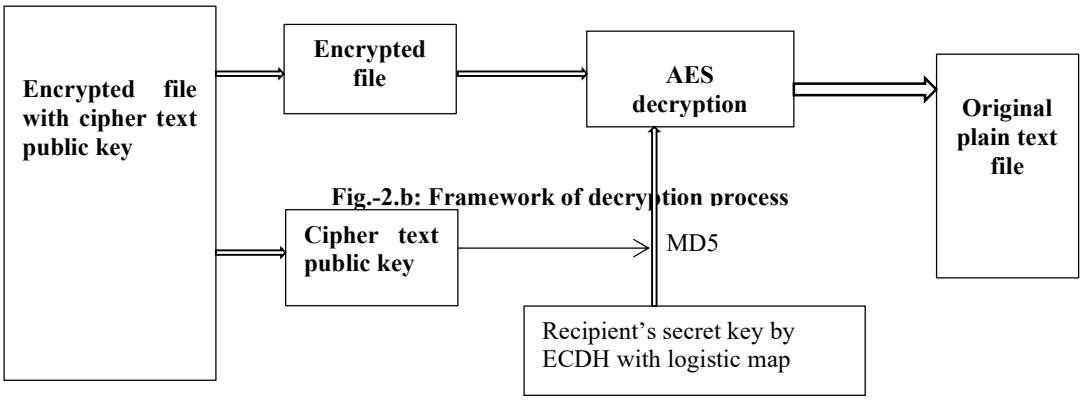


Fig.-2.b: Framework of decryption process

The following steps are involved in the proposed hybrid data security framework.

1. At first ECC key pair i.e. public and private key is generated and exchanged between sender and receiver through ECDH algorithm.
2. Again, a pseudorandom number is generated by logistic map and then XORed with ECC private key to produce a shared ECC public key.
3. Then, this shared key is converted to AES 256 bit secret key through MD5 hashing technique and the input text file is encrypted by AES 256 bit secret key.
4. After that sender transmits the encrypted file with cipher text public key randomly generated through ECDH algorithm to the receiver end via insecure channel.
5. Receiver receives the encrypted file and calculates ECC shared key by ECDH key exchange protocol and chaos based logistic map technique.
6. Then, the obtained shared ECC key is converted to AES 256 bit secret key through MD5 hashing technique.
7. Finally, the encrypted file is decrypted by AES 256 bit secret key to obtain an original text file at the receiver end.

Now, the following phases with techniques which are involved in our proposed hybrid data security system in implementing are explained as follows:

A. ECC key pair generation phase

Subject to the higher security at smaller key size, the elliptic curve E over field F_p is defined by Weierstraß equation as [10]:

$$E: y^2 = x^3 + ax + b \ mod \ p \qquad \text{Eq. - 1}$$

Where $a, b \in F_p$, and ρ is a prime number and the characteristic of the field F_p is not 2 or 3. The discriminant of the curve is $-16(4a^3 + 27b^2)$. The parameters of the curve brainpoolP256r1 [11] is given in Table-1.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Table-1: The brainpoolP256r1 curve parameters

Parameters	Values
p	A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
A	7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
B	26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
X	8BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262
Y	547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
Q	A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
H	1

Now, ECC key pair is generated through Elliptic-Curve Diffie-Hellman key exchange protocol between sender and receiver over an insecure channel. Assume two secret (private) numbers d_a and d_b in respect of sender and receiver. Key exchange with ECC generator point G over an insecure channel the values $Q_a=(d_a * G)$ (sender's public key) and $Q_b=(d_b * G)$ (Receiver's public key) and $[(d_a * G) * d_b = (d_b * G) * d_a]$ is the derived secret key.

The implementation steps of ECC key pair derivation by ECDH protocol are as follows [12, 13]:

1. Sender choose a random number d_a and computes $Q_a= d_a * G$
2. Receiver choose a random number d_b and generates $Q_b=d_b * G$
3. Sender and receiver exchange their public keys i.e. Q_a and Q_b through the insecure channel
4. Sender calculates sharedKey (K) = $d_a * Q_b=d_a * (d_b * G)$
5. Receiver calculates sharedKey (K') = $d_b * Q_a=d_b * (d_a * G)$
6. Now both sender and receiver have the same sharedKey == $d_a * Q_b == d_b * Q_a$

B. Pseudorandom number generation phase

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Chaos theory is a nonlinear, complicated dynamical system and the outputs of this system are highly dependent on the initial features, and conditions, so they are very random-like and highly unpredictable and non-deterministic [14]. In this context, we have generated a pseudorandom number through logistic map system. The logistic map is a one-dimensional discrete-time map that has been widely used in data security and secure communication due to its complex dynamic nature.

The logistic map is defined by the following equation [15]:

$$x_{n+1}=rx_n(1-x_n), \text{ where } n=0,1,2,3\ldots\ldots\ldots..\text{Eq.-2}$$

Here, 'r' is the system or control parameter and initial value of the system is set to $x_0[0<x_0<1]$.

When the value of 'r' is set to 4, then the logistic map goes into chaotic state. The generated logistic map after 500 iterations is given below the figure.

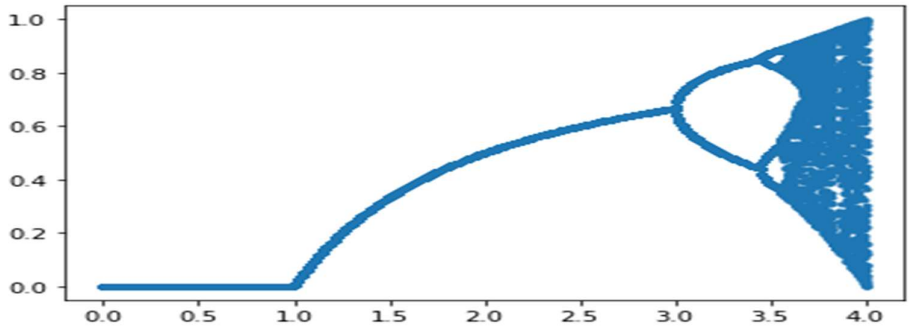


Fig.-3: Logistic Chaotic map

C. AES encryption and decryption phase

National Institute of Standards and technology (NIST) developed the AES algorithm (also known as the Rijndael algorithm) in 2000 to introduce a powerful symmetric block cipher algorithm that takes plain text with blocks of 128 bits and converts them to cipher text through the keys of 128, 192, and 256 bits respectively [16]. We have chosen AES 256 bit encryption technique in the proposed work for encrypting the input files. This supports the largest bit size and is practically non-breakable by brute force attack based on modern computing power, since the AES algorithm is considered secure and faster one in the worldwide. The following table shows that possible key combinations.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Table-2: Possible key combinations to crack by brute force attack [17]

Key Size	Possible Combinations
1 bit	2
2 bits	4
4 bits	16
8 bits	256
16 bits	65536
32 bits	4.2×10^9
56 bits (DES)	7.2×10^{16}
64 bits	1.8×10^{19}
128 bits (AES)	3.4×10^{38}
192 bits (AES)	6.2×10^{57}
256 bits (AES)	1.1×10^{77}

With AES 256-bit key, an intruder would need to try 1.1×10^{77} different possible combinations to crack the right one, that's why it makes more secure the encryption process.

For AES encryption, firstly, data is divided into blocks of 128 bits and then it undergoes the following steps [18]:

Step-1: AES key expansion, which creates new round key for each subsequent round of encryption using Rijndael's key schedule.

Step-2: AddRound key, in which the initial round key is added to the mix of data which has been divided.

Step-3: Substitute Bytes Transformation, which substitutes a byte in the state to another byte based on the Rijndael S-box substitution box [19].

Step-4: ShiftRows Transformation, which operates on each row of the divided data as the first row only one byte is moved to the left. The second row is moved two bytes to the left and third row is moved three bytes to the left.

Step-5: MixColumns Transformation, which multiplies each row of a pre-defined matrix with the columns of divided data and generate a new code block.

Step-6: AddRound key, in which another round key is added to the MixColumns.

After this initial round, the process is again repeated nine, 11, or 13 times, depending on AES key length of 128 bits, 192 bits, or 256 bits. AES encryption algorithm provides the best

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

security so that it relies on a number of rounds and inside each round comprise of four sub-steps (Step-3 to step-6).

In AES decryption, receiver one decrypts the received encrypted file using provided shared ECC public key and retrieves the original text. Here, decryption process involves reversing all the steps taken in encryption process and last round consists of three inverse functions such as InvShiftRows, InvSubBytes, and AddRoundKey [16].

5. EXPERIMENTS AND PERFORMANCE ANALYSIS

Jupiter notebook IDE and python 3.8 with tinyec, pycryptodome packages are used for the implementation of our proposed work. For experiment, the several data sets named as amazon_vfl_reviews [20], DataCoSupplyChainDatase [21], goodsdaily [22], NFT_tweets [23] and sales_test [24] are taken in the form of .xlsx files. Then, these files are converted into text files to perform the execution speed as well as security performance analysis in efficiently.

5.1 Execution Speed Performance Analysis

In SCM, a large amount of data is generated through IoT based resource constrained applications and also transferred to the different levels of SCM working flows. Hence, minimal execution time as well as higher throughput regarding encryption and decryption process is very much required for resource constrained IoT applications or sensor devices so that it will improve the efficiency and strength of the system. Based on experiment, we have represented the encryption time (EnTime) and decryption time (DecTime) with throughput of our taken dataset files in the following Table-2. Here, encryption throughput (EnTp) and decryption throughput (DecTp) are computed based on input text file (kb) which is divided by total encryption time (ms) and by total decryption time (ms) respectively and the corresponding equations are listed below [4]:

$$\text{Encryption Throughput (Kb/ms)} = \frac{\sum(Input\ file)}{\sum(Encryption\ time)} \qquad \text{Eq.-3}$$

$$\text{Decryption Throughput (Kb/ms)} = \frac{\sum(Input\ file)}{\sum(Decryption\ time} \qquad \text{Eq.-4}$$

Table-3: Encryption and decryption time with throughput of dataset files

Datasets with size (Kb)	EnTime(ms)	DecTime(ms)	EnTp(Kb/ms)	DecTp(Kb/ms)
amazon_vfl_reviews (778)	96.804	78.128	8.036	9.958
sales_test (1,498)	104.996	82.502	14.267	18.157
NFT_tweets (5,225)	140.625	96.264	37.155	54.27

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Goodsdaily (29,956)	410.154	308.392	73.035	97.135
DataCoSupplyChainDataset (93,935)	1142.773	893.533	82.199	105.127

The Table-3 clearly depicts that our proposed technique takes very less encryption and decryption time with high throughput according to the varying file size in Kb.

5.2 Security performance with Entropy analysis

In cryptography, information entropy refers to the measure of randomness in a system. If the system is more random, the system is less predictable and it's more entropy [15]. In our proposed work, entropy value is calculated to measure the security strength of the encrypted text based on the following equation.

$$Entropy = -\sum_{i=1}^{m} p(i) \log_2 p(i) \qquad \text{……Eq.-5}$$

Table-4: Entropy values of encrypted files with corresponding input files

Datasets	Entropy	
	Input file	Encrypted file
amazon_vfl_reviews	5.02	5.99
sales_test	4.56	5.99
NFT_tweets	5.69	5.99
Goodsdaily	4.22	5.99
DataCoSupplyChainDataset	5.34	5.99

From the Table-4, it can be say that our proposed work is robust and secure because the entropy values of each encrypted file are higher than the corresponding input files.

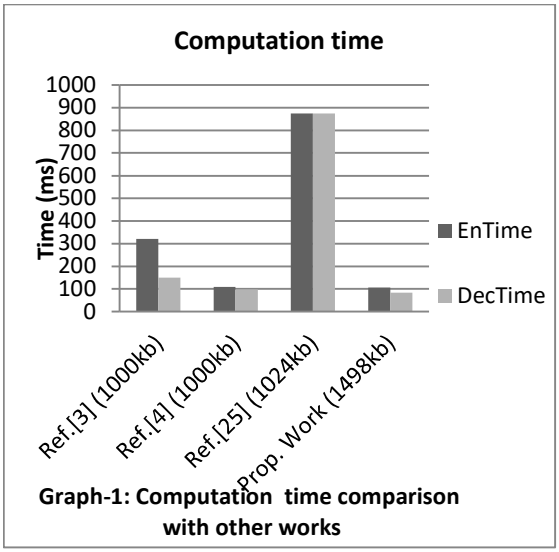
5.3 Comparative analysis

Based on experiment, performance analysis compared to other existing works is shown in the following Table-5 and it also plotted graphically in the Graph-1 and Graph-2 respectively. Here, "EnTime", DecTime", "EnTp" and "DecTp" refer Encryption time, Decryption time, Encryption Throughput and Decryption Throughput respectively.

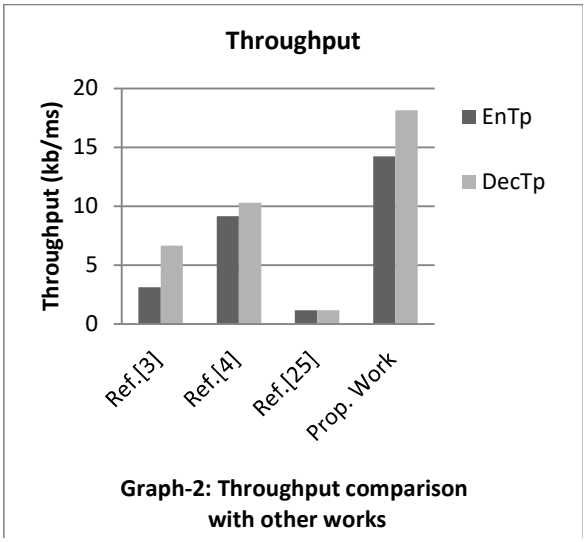
Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Table-5: Comparative analysis with other works

Technique	File size (Kb)	EnTime(ms)	DecTime(ms)	EnTp(Kb/ms)	DecTp(Kb/ms)	Entropy
Ref.[3]	1000	320	150	3.125	6.666	NA
Ref.[4]	1000	109	97	9.17	10.30	NA
Ref.[25]	1024	874.23	874.23	1.17	1.17	NA
Proposed work	1,498	104.99	82.50	14.26	18.15	5.99



Graph-1: Computation time comparison with other works



Graph-2: Throughput comparison with other works

In this work, a hybrid encryption technique is proposed through ECC key pair generation with

In this work, a hybrid encryption technique is proposed through ECC key pair generation with chaos based logistic map equation and AES 256 bit encryption algorithm. The ECC key pair is generated and exchanged between sender and receiver based on Elliptic-Curve-Diffie-Hellman (ECDH) algorithm using brainpoolP256r1 curve. Then the generated ECC secret key is XORed with chaotic pseudorandom number key which is generated by logistic map and also produces a shared ECC key to increase the randomness of the keys so that our proposed system satisfy the authenticity, integrity and confidentiality security requirements regarding the applications and services in IoT based SCM. After that the value of the shared ECC key is passed to MD5 secure hash function to produce 256 bit AES secret key and used in encryption

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

and decryption purpose. The sensitive information is encrypted by produced AES secret key before it sending to the different required levels of SCM through IoT network and it helps to protect the IoT based SCM applications and services in securely from the security attacks like brute force attack as well as side channel attacks. Regarding the performance comparison, from Graph-1 and Graph-2 it is clearly observed that the computation time based on encryption and decryption time is lighter than other existing works and further, encryption and decryption throughputs are also high compared to other related works. Hence, our proposed technique is more suitable for IoT based resource constrained devices or applications where faster implementation with less memory consumption is required to increase the embedded efficiency of the system.

Again, we have computed the entropy values of the taken datasets and their corresponding encrypted files to measure the randomness of the system. This is shown in the Table-4 and it is observed that the entropy of the encrypted files is more compared to the entropy of the original input files and hence, our proposed hybrid encryption technique is entropically secure as it is computationally infeasible for intruders to retrieve any information from the encrypted files. Therefore, our proposed approach based on the performance of execution speed and security strength through entropy measurement is more computationally fast and secure compared to other related existing techniques.

6. CONCLUSION

Nowadays, many business companies are very much interested to the use of IoT based applications in SCM in improving the efficiency of the business and hence the security concerns are also increased in simultaneously. In this regard, a secure security framework for transferring sensitive information or data to the different levels of SCM through IoT network is required to protect. Hence, we have proposed a hybrid ECC-AES encryption technique for data security in IoT based SCM. In this work, ECDH key exchange protocol using brainpoolP256r1 curve is implemented to generate ECC key pair and the secret key is XORed with the key generated through chaotic logistic map equation and then ECC key is shared between sender and receiver. Here, logistic map is used to increase the randomness of the secret key. Again, AES 256 bit secret key is generated through MD5 hashing technique to encrypt the text data before transferring among the different levels of SCM through IoT network. The required data can be downloaded and decrypted at the receiver point in analyzing or classifying the data for future prediction in accurately. The experiment has been conducted through five taken text data files and the performance analysis is carried out based on computation time as well as security strength. According to performance analysis, our proposed hybrid encryption approach is very fast and secure compared to other related works. Hence, it can be concluded that our proposed technique is more appropriate in applying to the IoT based resource constrained applications or devices in SCM where faster implementation with fewer resources is required.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

REFERENCES

- Abdullah, A. M. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Cryptography and Network Security, 03-13.
- Abu-Faraj, M. A. M., & Alqadi, Z. A. (2021). Using Highly Secure Data Encryption Method for Text File Cryptography. International Journal of Computer Science & Network Security, 21(12), 53-60.
- Ashton, K. (2009) That Internet of things thing, RFID Journal. Retrieved from://http://www.rfidjournal.com/articles/view?4986.
- ATP (2019). Secure your data with AES-256 encryption. blog. Retrieved from //https://www.atpinc.com/blog/what-is-aes-256-encryption
- Daniel, B. (2021). What Is AES Encryption?. blog. Retrieved from "//https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered//".
- Farooq, M.J. and Zhu, Q. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead. arXiv:1908.07828v1
- Github. Practical-Cryptography-for-Developers-Book. Retrieved from //https://github.com/nakov/Practical-Cryptography-for-Developers Book/blob/master/ asymmetric -key-ciphers/ecdh-key-exchange.md
- ITconvergence, The Role Of IoT In Supply Chain Management. Retrieved from //https://www.itconvergence.com/blog/the-role-of-iot-in-supply-chain-management/
- Jian, M., Cheng, Y. & Shen, C. (2019). Internet Of Things (IOT) Cybersecurity based on the Hybrid Cryptosystem. International Conference on Advanced Communications Technology, 176-181.
- kaggle. DataCo Smart Supply Chain for Big Data Analysis. Retrieved from //https://www.kaggle.com/datasets/shashwatwork/dataco-smart-supply-chain-for-big-data-analysis.
- Kaggle. Indian Products on Amazon. Retrieved from //https://www.kaggle.com/datasets/nehaprabhavalkar/indian-products-on-amazon.
- Kaggle. NFT Tweets. //https://www.kaggle.com/datasets/mathurinache/nft-tweets.
- Kaggle. Supply chain CEL dataset. Retrieved from //https://www.kaggle.com/datasets/annelee1/supply-chain-cel-dataset.
- Kaggle. Supply_Chain. Retrieved from //https://www.kaggle.com/datasets/mylife97/supply-chain.
- Lochter & Merkle (2010). Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Informational. /https://datatracker.ietf.org/doc/html/rfc5639#page-11.
- Mehrabi, M. A., & Jolfaei, A. (2022). Efficient Cryptographic Hardware for Safety Message Verification in Internet of Connected Vehicles. ACM Transactions on Internet Technology (TOIT).
- Mousavi, S.K. · Ghaffari, A., Besharat, S. & Afshari, H. (2020). Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Journal of Ambient Intelligence and Humanized Computing. //https://doi.org/10.1007/s12652-020-02303-5

- Mukherjee, S., Hasan, M., Chowdhury, B. & Chowdhury, M. (2011). Security of RFID Systems - A Hybrid Approach. 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. DOI 10.1109/SNPD.2011.40
- Purswani, J., Rajagopal, R., Khandelwal, R., & Singh, A. (2020). Chaos theory on generative adversarial networks for encryption and decryption of data. In Advances in Bioinformatics, Multimedia, and Electronics Circuits and Signals, 251-260.
- Ragab, A., Selim, G., Wahdan, A. & Madani, A. (2019). Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices. SpaCCS 2019 Workshops, LNCS 11637,5–19.
- Rajesh, S., Paul, V., Menon, V. G. and Khosravi, M. R. (2019). A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. Symmetry, 11, 293, 01-21. doi:10.3390/sym11020293
- Rehman , S., Bajwa, N. T., Shah, M. A., Aseeri, A. O. and Anjum, A. (2021). Hybrid AES-ECC Model for the Security of Data over Cloud Storage. Electronics, 10, 2673, 2-20. //https://doi.org/10.3390/electronics10212673
- Saepulrohman, A., Denih, A., & Bon, A. T. (2020, August). Elliptic curve Diffie-Hellman cryptosystem for public exchange process. In The 5th NA International Conference on Industrial Engineering and Operations Management,1-6.
- Wang, L. & Cheng, H. (2019). Pseudo-Random Number Generator Based on Logistic Chaotic System. Entropy, 21, 960, 1-12.
- Wikipedia. Rijndael S-box. Retrieved from "//https://en.wikipedia.org/wiki/Rijndael_S-box".

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/