Privacy- Preservation and Network Security Using Multi-Keyword Ranked Search

[1]M.Nagaraju Naik. [2]Prof.M. Padmavathamma
[1]Research Schlaor, [2]Research Supervisor
[1,2]Department of Computer Science
S V University, Tirupati

Abstract: With the development of emerging technologies such as big data, IoT and cloud computing, innovative solutions for simpler communication are provided. Besides, the advancements serious issues of threats and attacks to data are manipulated each time. Various intrusion detection methods are evolved in aspects of detecting the common network attacks. Attack detection technologies play a potential role in securing the data and other essentials form an intrusion or an attack. These attacks provides consequences such as heavy data breaches and data loss resulting in complete data unavailability. Many such approaches have been carried out in detecting and in classifying the attack over the networks. But these approaches are associated with several complexities such as lower accuracy rates, high computational complexity. Further challenges are laid in cases of less detection rates of feature space, less recognition to encrypted data and detecting only known attacks. Considering these laybacks, the DL approaches are one of the promising solutions in providing remarkable outcomes in both attack detection and classification. These are viable in producing remarkable outcomes in case of accuracy rates, less complexity, and faster detection rates.

I. INTRODUCTION

As technology advances effortlessly into every single corner of day-to-day life, protection and privacy are becoming indivisibly entwined. The security and privacy of users became the initial concern due to IoT association in several applications. Increasing fiery pace of cyber threats makes the existing security and privacy measures as an inadequate one. On the other hand, the unsettled concern is how to protect the collected data privacy in an efficient way at the time it is processed and managed. Cryptography is a extensively employed strategy to protect the data in the free cloud. It enables the customers to employ the mutual cloud adminstration in an effective and reliable way since the complete data is protected. The cryptography then converts the normal text into an unreadable format and thereby limits the data view while transferred or relocated. The encryption helps to prevent the sensitive data from getting into the hands of the attacker. Also, the encytption protests the privacy of the subtle data. While employing the encryption process, it is vital to preserve the encryption keys in a secure way. For the purpose of safeguarding the data, several encryption algorithms are presented. AES is a highly preferred symmetric key block cipher. The calculation of AES is performed in bytes; hence, it employs the one hundred and twenty eight bits plaintext block as sixteen bytes as the matrix one. In the AES algorithm, premutations and substitutions are executed. The sum of transformation rounds employed for encryption process is determined by the size of key used for the AES cipher. The ECC is a robust and rapid cryptographic technique for data privacy and public key cryptomethod. The ECC employs two keys for encryption, namely private and public keys. This in turn, surges the security. Although the AES is employed for encryption, the ECC algorithm is more protected than the AES algorithm. The ECC employs both the public and private key whereas, AES employs only the single key. Because of that only the admin can login to the system directly, while the remaining users are required to register in the cloud system to log in. The hybrid proposed model (ECC and AES) will execute in same way to minimize the size of the key. By employing ECC, public key is created, and the encryption and decryption are performed employing the AES algorithm. Therefore, this minimizes the cost of computation and improves data security.

II. PROPOSED METHODOLOGY

The study aims to accomplish privacy preservation and Network Security by Multi-Keyword Ranked Algorithm. The present study proposes certain processes as shown in figure 1. Primarily, the Cybersecurity KddCup99 dataset is loaded. And then the loaded dataset is pre-processed. Data pre-processing involves several features, like removing the redundant noises and reducing the column and filling the missing values. After pre-processing, encryption process is done for the multi keyword ranked search by employing the hybrid Elliptical Curve Cryptography (ECC) and Advanced Encryption Standard (AES) algorithm. Encryption process is done to safeguard the confidential data. Followed by that, the data is split into 80% and 20%, in which 80% of the data is trained and the remaining 20% is tested.

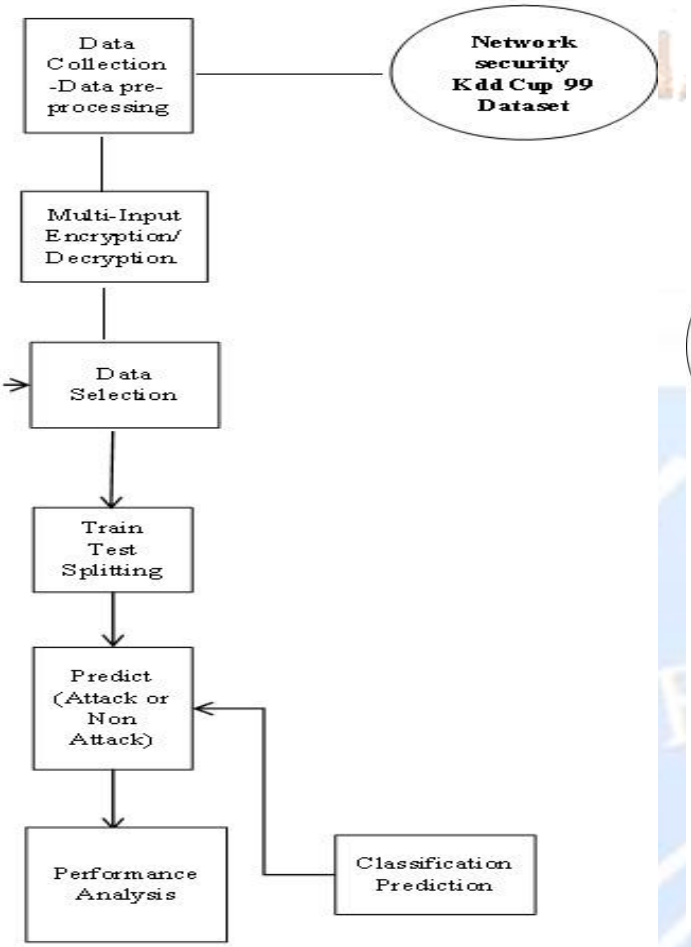

Figure 1 Proposed research flow

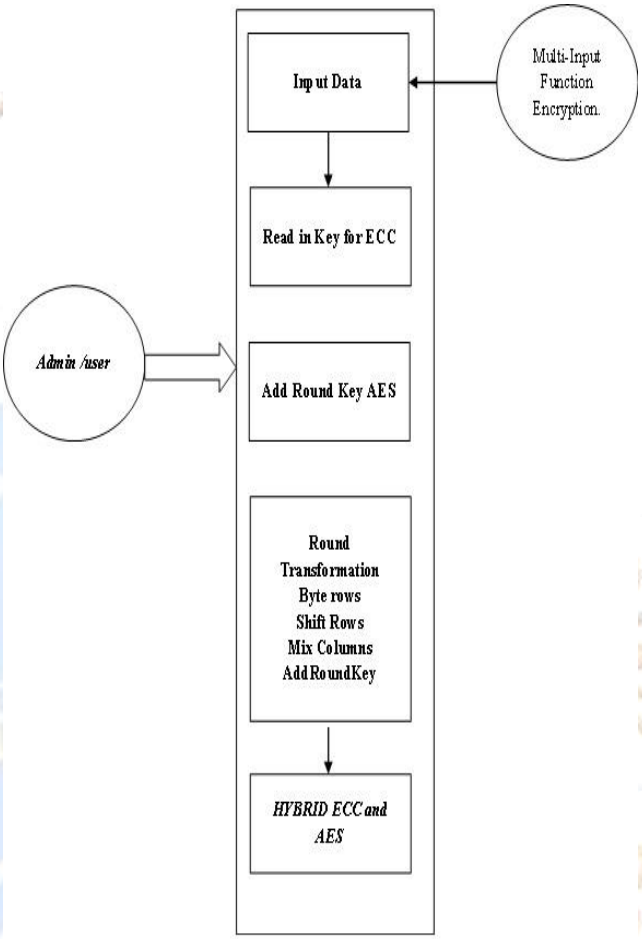

Figure 2 Multi-Keyword Ranked Search Over Encrypted Data Share—Hybrid ECC and AES Algorithm

As depicted in the Figure 2, the encryption stages are provided via the input data.

III. HYBRID ECC AND AES ALGORITHM

ECC is a key-centred method to execute data encryption. It focuses on public and private keys to execute encryption and decryption. ECM is linked with cryptography, named as ECC, to perform key-cryptography. It offers a safe way to implement cryptographic operations, namely encryption, key exchange and digital signatures. Also, ECC possesses a discrete standard up-to-date as a well-known technique that could be understood in exponential period. And its security attains from the EC algorithm that is the Discrete Logarithm Problem (DLP) in the collection presented by focusing on EC on limited area. This leads to extraordinary reduction in size of the key in order to obtain alike stages of security.

In this study ECC is proposed due to its smaller key size because it provides superior security level when compared with other algorithms. Also, ECC can provide a security level that needs fewer computing resources to decrypt and encrypt data.

AES is a symmetric encryption algorithm. It is executed in hardware and software all over the world to encrypt sensitive data. AES is the standard for electronic data encryption. It is a symmetric block cipher system. This employs an exchange or network replacement. The variable are data key length and block length. It is widely used security protocol for wide range of applications namely, encryption information storage, e-business, financial transactions and wireless communication. In this study, AES is implemented to protect the classified data. The fundamental benefit of AES is the variety of key lengths available. The length of the key used to protect the communication directly correlates to how long it takes to break an encryption technique.

On the other hand, AES starts its function on data bytes rather than data bits. For example, the block size is 128-bits and the cipher processes the input of 16 bytes (128 bits) at precise time. For computing every round key, scheduled approach is employed. The primary key is employed for generating numerous round keys that are then employed in encryption round. The AES algorithm has numerous advantages.

It subsists as a classic security protocol employed for numerous applications. It appears to be not possible to hack private data. An example, for 128 bit, 2^{128}attempts are needed for breaching. And this procedure makes it composite in hacking, and therefore, it subsists as a benign etiquette. It is a sort of cipher-text that uses block cipher. The AES algorithm is employed in the study due to its easy application and its time compatibility.

Figure 3.3 displays the hybrid ECC and AES algorithm architecture. The proposed ECC-AES algorithm aids in creating efficient and improved cryptographic method. Due to the giant size of the AES, it is slightly slower than the ECC-AES. Although the hybrid method allows minimized key size and a rapid security method to secure data. Due to small key size, AES employs ECC to execute encryption, reduce the size of the key and improve in enactment. In such conditions, ECC employs decryption and encryption values to reduce the key size and improve a safe system. Besides, ECC appears to be an appropriate method for use with AES for achieving safe data from an unauthorized usage. Once setting the key size, ciphertext creates decryption and encryption of data. The Mutual impact of ECC-AES is appropriate to achieve a secured system, and the complete process is shown in algorithm 1.

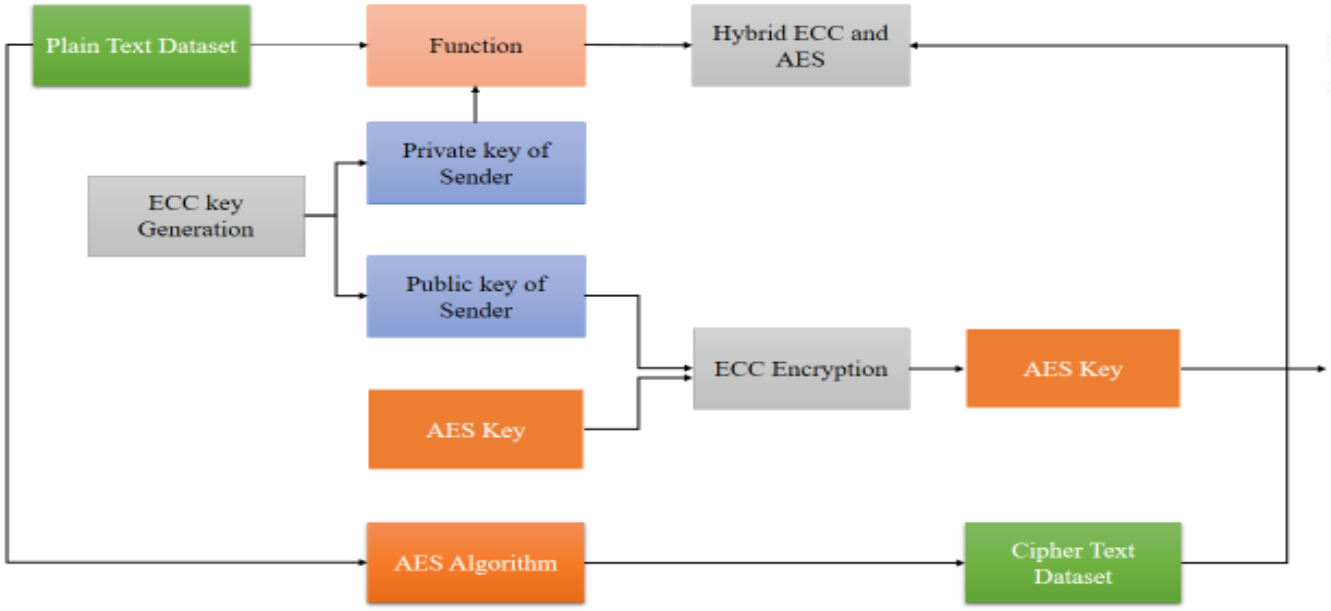

Figure 3 Hybrid ECC and AES algorithm architecture

Algorithm 1 -Hybrid ECC and AES algorithm

Key expansion function
For i=0 to 3
$K_i \leftarrow key_{4i} + key_{4i+1} + + key_{4i+2} = key_{4i+3}$
If (i mod4 ≠0) $k_i \leftarrow k_{i-1} \oplus K_{i-4}$
Subword(rotword(k_{i-1}*))*

Encryption code AES -64
Encryption function (input_block[16],output_block[16])
encrypt(input_block,S_e*)*
s←addroundkey(S_e*,k[0..3])*
$\sum_{round=1}^{10} Se \leftarrow subbytes(s), Se \leftarrow shiftrows(s)$
If (round≠0), S_e *←mixcolumn(*S_e*)*
S_e *←addroundkey(*S_e*,k[4 x round, 4 x round +3])*
encrypt(s,output_block)

Encryption code ECC-128
Encryption function encrypt $(s_c, output\_block[16])$
encrypt (input_block, s_c*)*
$s_{c_i} \leftarrow$ *addroundkey (*s_c*, k [0...3])*
$\sum_{round=1}^{10} Sce \leftarrow subbytes(s_{c_i}), Sce \leftarrow shiftrows(s_{c_i})$
If (round≠0), Sc_e *←mixcolumn (*S_e*)*
Sc_e *←addroundkey (*Sc_e*, k [4 x round, 4 x round +3])*
Encrypt (s_{c_i}*, output block)*

Decryption code ECC -128
Decryption function $(s_{cd}, output\_block[16])$
Decrypt (input_block, s_{cd}*)*
s_{cd} *←addroundkey (*s_{cd}*, k [0...3])*
$\sum_{round=1}^{10} Sd \leftarrow inv\_subbytes(s_{cd}), s_{cd} \leftarrow inv\_shiftrows(s_{cd})$
If (invround≠0), s_{cd} *←mixcolumn (*s_{cd}*)*
s_{cd} *←addroundkey (*s_{cd}*, k [4 x invround, 4 x invround +3])*
Decrypt (s_{cd}*, output_block)*

Decryption code AES-64
Decryption function (output_block[16],input_block[16])
decrypt(input_block,S_d*)*
S_d *←addroundkey(*S_d*,k[0..3])*
$\sum_{round=1}^{10} Sd \leftarrow inv\_subbytes(Sd), Sd \leftarrow inv\_shiftrows(Sd)$
If (invround≠0), S_d *←mixcolumn(*S_d*)*
S_d *←addroundkey(*S_d*,k[4 x invround, 4 x invround +3])*
decrypt(S_d*,output_block)*

IV. Conclusion

ECC-AES provides superior security with a smaller key size when compared to other cryptographic methods. Due to the decreased key size, it optimizes memory usage and lowers computational complexity. Therefore, by employing a medium sized key, a great level of data safety can be attained.

References

[1] R. Walia, N. Oberoi, A. Kumar, and G. Singh, "Digital Fingerprint and Security Aspects in Internet of Things Against Social Engineering Using Advanced Digital Forensics," *Test Engineering and Management*, vol. 83, pp. 4914-20, 2020.

[2] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data*, vol. 7, pp. 1-29, 2020.

[3] J. Deepika, C. Rajan, and T. Senthil, "Security and privacy of cloud-and IoT-based medical image diagnosis using fuzzy convolutional neural network," *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1-17, 2021.

[4] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions," *Journal of Cloud Computing*, vol. 10, pp. 1-34, 2021.

[5] J. Singh and J. Singh, "A survey on machine learning-based malware detection in executable files," *Journal of Systems Architecture*, vol. 112, p. 101861, 2021.

[6] Ö. Aslan, M. Ozkan-Okay, and D. Gupta, "A review of cloud-based malware detection system: Opportunities, advances and challenges," *European Journal of Engineering and Technology Research*, vol. 6, pp. 1-8, 2021.

[7] M. Naseri, J. Hayes, and E. De Cristofaro, "Local and central differential privacy for robustness and privacy in federated learning," *arXiv preprint arXiv:2009.03561*, 2020.

[8] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices," *IEEE Internet of Things Journal*, vol. 9, pp. 3930-3944, 2021.

[9] R. HAMZA and M.-S. DAO, "Privacy-preserving deep learning techniques for wearable sensor-based Big Data applications," *Virtual Reality & Intelligent Hardware, XXXX, XX (XX)*, pp. 1-13, 2022.

[10] P. Dixit and S. Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Computer Science Review*, vol. 39, p. 100317, 2021.

[11] H. Zhu, R. Wang, Y. Jin, K. Liang, and J. Ning, "Distributed additive encryption and quantization for privacy preserving federated deep learning," *Neurocomputing*, vol. 463, pp. 309-327, 2021.

[12] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 53, pp. 1-37, 2020.

[13] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet of Things Journal*, vol. 8, pp. 9463-9472, 2020.

[14] O.-A. Kwabena, Z. Qin, T. Zhuang, and Z. Qin, "Mscryptonet: Multi-scheme privacy-preserving deep learning in cloud computing," *IEEE Access*, vol. 7, pp. 29344-29354, 2019.

[15] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 1963-1971, 2019.

[16] J. Zhao, K. Mao, C. Huang, and Y. Zeng, "Utility optimization of federated learning with differential privacy," *Discrete Dynamics in Nature and Society*, vol. 2021, pp. 1-14, 2021.

[17] Ö. Aslan, M. Ozkan-Okay, and D. Gupta, "Intelligent behavior-based malware detection system on cloud computing environment," *IEEE Access*, vol. 9, pp. 83252-83271, 2021.

[18] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Transactions on Network and Service Management*, vol. 16, pp. 924-935, 2019.

[19] V. Rey, P. M. S. Sánchez, A. H. Celdrán, and G. Bovet, "Federated learning for malware detection in iot devices," *Computer Networks*, vol. 204, p. 108693, 2022.