Madhudhara.V, 2024, 12:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Privacy-Preserving Cyber Forensic Analysis Using Encrypted Feature Vectors for Secure Investigations

Madhudhara.V, Sivapriya. R, Sudharshini. C, D. Suganthi, J Mythili, Dr. N. Prabhu
Department of Computer Science with Cognitive Systems,
PSGR Krishnammal College for Women, Coimbatore, India.

Abstract- Securing sensitive data while allowing forensic analysis is becoming more important as digital data use rises. Machine learning-based cyber forensic investigations rely on feature vectors, which quantify digital data. However, these vectors typically include important data that must be securely stored. This work uses complex cryptographic methods including AES, RSA, and homomorphic encryption to encrypt feature vectors. Cyber forensics analyse encrypted routes to find abnormalities, track digital footprints, and uncover security breaches while protecting data. This innovation improves cybersecurity by allowing secure investigations without losing secrecy using encrypted forensic analysis. Results show that encrypted feature vectors may be handled privacy-preserving, retaining data integrity and investigative accuracy. In cyber forensics, this method affects malware detection, intrusion detection, and safe digital evidence management.

Keywords- Cyber Forensics, Encryption, AES, feature vectors, Cyber Security

I. INTRODUCTION

Encrypting feature vectors may enhance security by preventing unauthorised access to vital information. It is essential to recognise that data encryption may negatively impact the performance of processing and analytical operations. Processing encrypted feature vectors requires specialist methods that can operate on encrypted data without revealing its contents. Homomorphic encryption is a method that permits computations on encrypted data without the need of preceding decryption. However, homomorphic encryption may be resource-intensive and may not be suitable for many applications [8]. An alternate approach to assessing encrypted feature vectors employs secure multi-party computing (MPC) protocols, allowing several parties to jointly assess a function on their secret inputs while preserving the confidentiality of those inputs from each other. MPC protocols provide the implementation of various operations on encrypted data, such as clustering and classification, while maintaining data privacy. In addition to encryption, it is essential to ensure that the processing and analysis of feature vectors take place inside a secure environment. This may include implementing access limitations, monitoring system activity for aberrant behaviour, and introducing supplementary security measures to protect against cyber assaults [11]. Encrypting feature vectors may enhance security; nevertheless, it is essential to thoroughly assess the performance and computational requirements of the chosen encryption technique, as well as other security procedures needed to ensure the system's overall security [6].

II. ENCRYPTING FEATURE VECTORS FOR CYBER FORENSICS

Encrypting feature vectors for cyber forensics is advantageous for protecting sensitive information from unauthorised access. Feature vectors are numerical representations of data used for the study and categorisation of information across several fields, including cyber forensics. The

Advanced Encryption Standard (AES) is a widely used encryption method in cyber forensics. It is a symmetric encryption technique, indicating that the same key is used for both encryption and decryption. The key length may vary from 128 to 256 bits, with longer lengths providing superior encryption strength. To encrypt a feature vector using AES, the vector is first converted into a binary representation. The binary data is then encrypted using the AES method and a secure key [13]. The resulting ciphertext is thereafter stored or sent securely [4]. The receiver uses the same secret key and the AES algorithm to decrypt the ciphertext, reverting the data to its original form. The decrypted feature vector may then be used for analysis and classification in cyber forensics. It is essential to acknowledge that the encryption of feature vectors may negatively impact the accuracy of certain analytical procedures reliant on the original data [8]. Moreover, it is essential to adequately preserve and protect the secret key used for encryption and decryption.

III. DECRYPTED FEATURE VECTOR IN CYBER FORENSIC

In cyber forensics, a feature vector is a compilation of numerical values that denote distinct qualities or aspects of digital evidence, including files or network activity. These feature vectors may be used to train machine learning models for the automated classification or analysis of digital evidence [12]. A decrypted feature vector denotes a feature vector that has been restored from encrypted data. Encryption is often used to safeguard sensitive information during transmission or storage; nevertheless, in the realm of cyber forensics, encrypted data may complicate the analysis of digital evidence [1]. If investigators successfully recover an encrypted feature vector, they may decode it to get the original feature vector, which can assist in their research. This may include juxtaposing the feature vector with established patterns or using it to build machine learning models to facilitate the identification or categorisation of digital evidence.

Table 1. Performance Comparison of Encryption Algorithm

Encryption Algorithm	No. of Users (ms)	Execution Time (ms)
AES algorithm	30	4201
RSA algorithm	20	8504
Hormonic Encryption	40	7540

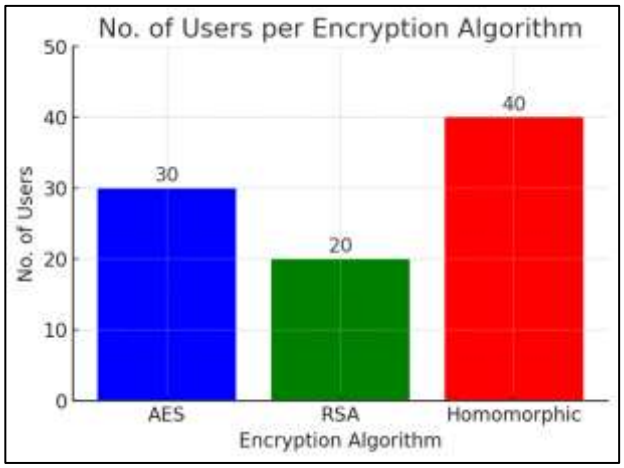

Figure 3. Execution Performance

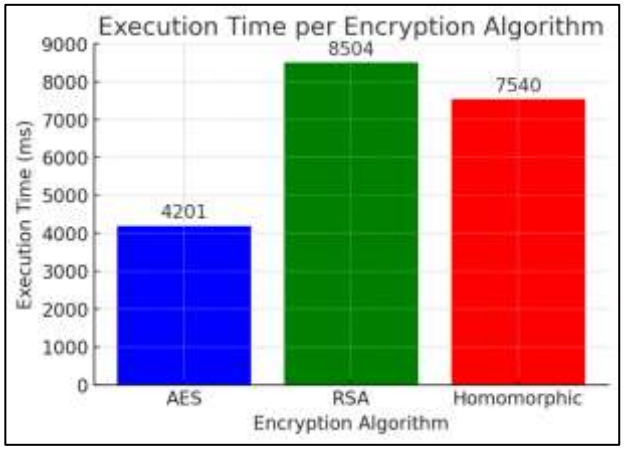

Figure 4. Execution Performance

Table 2. Probability of Forensic Relevance

No. of Users (ms)	Logged Users	Accessed Database	Crime Probability
145	140	135	5
50	48	45	7
90	85	82	45
320	25	7	15
40	30	10	22
15	10	6	10

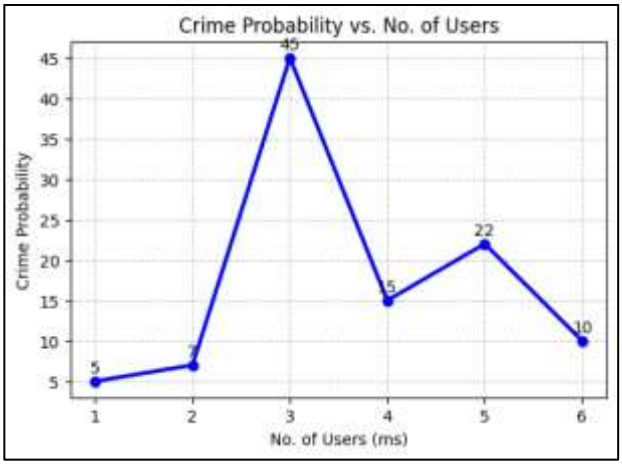

Figure 5. Probability of Forensic Relevance

V. CONCLUSION

The investigative system may get the MAC address using the supplied IP address. This utility identifies the physical address of a device and associates it with the matching IP address. The program displays the MAC address with user data, IP address, DNS, port number, community, system name, system type, and system details. The investigative procedure yields a compilation of MAC addresses associated with the user's computer hackers. Their associated IP addresses and DNS names are likewise enumerated. The MAC address will be sent to the cyber-crime unit to ascertain the physical location of the IP address. This leads to a reduction in the number of iterations required for evidence retrieval. The examination of criminal activity in relation to the likelihood of a threat. The AES and AESK encryption protocols are used to provide a secret key for the encryption and storage of user credentials or marks in the database.

REFERENCES

1. Cheng Yan. (2011) 'Cybercrime Forensic System in Cloud Computing, Department of Computer Science and Engineering', East China University of Political Science and Law, Shanghai, China, IEEE 2011
2. Do Hoon Kin and Hoh Peter In. (2008). 'Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics', 2008 International Conference on Information Security and Assurance (ISA), pp 193-198.
3. Feng-Yu Lin, Yeali S. Sun and Meng Chang Chen. (2014) Forensics Tracking for IP User Using the Markov Chain Model, Applied Mathematics and Information Sciences I.J., Vol 8 (3), pp 1343-1353
4. José Antonio Maurilio Milagre de Oliveira and Marcelo Beltrão Caiado. (2013) 'Best Practice and Challenges for Process Efficiency of Investigations and digital Forensics', The Eighth International Conference on Forensic Computer Science 2013, pp 1-9.
5. Mohsen Damshenas et al. (2012) 'Forensics Investigation Challenges in Cloud Computing Environments', International Conference on Cyber Security, Cyber Warfare and Digital Forensic (Cyber Sec
6. Adams R., Val Hobbs and Graham R. (2015) 'The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice', Digital Forensics, Security and Law I.J., Vol. 8(4), pp 234-238.
7. Vijayarani, S., Suganya, E., & Navya, C. (2021). Crime analysis and prediction using enhanced Arima model. Journal homepage: www. ijrpr. com ISSN, 2582, 7421.
8. Mohan H. S. and Raji Reddy A. (2011) 'Performance Analysis of AES and MARS Encryption Algorithms', Computer Science Issues I.J., Vol. 8(4), pp 1-6.
9. Mohan H. S. and Raji Reddy A. (2011) 'Performance Analysis of AES and MARS Encryption Algorithms', Computer Science Issues I.J., Vol. 8(4), pp 1-6.
10. Dr.J.Viji Gripsy, K.R.Kanchana, A Survey on Recent Secure Routing Techniques in Mobile Ad-Hoc Networks", International Journal of Future Generation Communication and Networking, Volume 13, Year 2020, Pages 594-602
11. Viji Gripsy.J, Kowsalya R, Banupriya C V, and Sathya R. 2024. Secured Data Transmission Using Pareto Optimization Based Lion Swarm Optimization and Double Encryption based Blowfish Algorithm in WSN. In Proceedings of the 5th International Conference on Information Management & Machine

Intelligence (ICIMMI '23). Association for Computing Machinery, New York, NY, USA, Article 23, 1–6. https://doi.org/10.1145/3647444.3647849