Journal of Namibian Studies, 35 S1 (2023): 1221-1238 ISSN: 2197-5523 (online)

Enhancing Security In Device-To-Device Communication Of 5G Networks Through Hybrid Method Using AES And Huffman Encoding

Chaithanya D.J.[1] , Dr. Anitha S.[2]

[1]Research Scholar ACS College of Engineering, Bangalore
Visvesveraya Technological University,
Belagavi - 590018
rcchaithudj@gmail.com
[2]Research Supervisor Professor, Dept. of BME,
ACS College of Engineering, Bangalore
Visvesveraya Technological University,
Belagavi - 590018
dranithasammilan@gmail.com

Abstract

D-2-D (Device to Device) communication is essential in 5th Generation communication networks for allowing communication between devices without transmitting data through the network infrastructure and it plays a major challenge in assuring the effectiveness and security of D-2-D (Device to Device) communication. In this research work, a hybrid method is proposed for the security and effectiveness of Device-to-Device communication in 5G networks by combining AES encryption with Huffman coding techniques and achieving enhanced security for D-2-D (Device to Device) communication while maintaining efficient data transmission. The AES method is known for protecting Device-to-Device (D2D) communication in 5th Generation networks. An effective security solution is provided by the AES algorithm for D-2-D (Device to Device) communication in 5th Generation networks, guaranteeing the secrecy of data exchanged between devices. This work enhances the privacy of D-2-D (Device to Device) communication, making it suitable for 5th Generation networks and it provides robust encryption of data while Huffman coding reduces the data size for efficient transmission using Python programming language.

Keywords— AES, Device to Device, security, Huffman coding.

I. Introduction

The Advanced Encryption Standard (AES) algorithm has emerged as a dependable response to these security issues for safeguarding D-2-D **(**Device to Device **)** [38]communication in 5G networks and is a symmetric encryption used for reliability and effectiveness in safeguarding sensitive data. The method used in encryption in D-2-D **(**Device to Device) communication adds another level of security by protecting the integrity and confidentiality of transmitted data. The main objective of this hybrid method is to propose the AES algorithm specifically for D-2-D **(**Device to Device) communication within the context of 5^{th} Generation networks [6][7]. The key concepts of the Advanced Encryption Standard (AES) algorithm are described using examples from D2D communication and are essential for secure D-2-D **(**Device to Device) communication in 5G networks and the significant use of a powerful encryption method like Advanced Encryption Standard (AES) [8][9]. The key distribution, key generation, encryption, and decryption operations compose the following components of the proposed Advanced Encryption Standard (AES) algorithm's technological implementation. This proposed work will focus on the performance and safety aspects of the AES algorithm in D2D communication scenarios for providing a few encryption modes [10]. Stakeholders in the 5G networks and it is difficult to guarantee the privacy and security of D-2-D **(**Device to Device) communication, though. Data interceptions and unauthorized access are serious issues that require attention [3][4][5]. The Advanced Encryption Standard algorithm has emerged as a dependable response to these security issues for safeguarding Device to Device communication in 5G networks. Advanced Encryption Standard (AES) is a symmetric encryption used for reliability and effectiveness in safeguarding sensitive data and this method used in encryption of D-2-D **(**Device to Device) communication adds another level of security by protecting the integrity and confidentiality of transmitted data. The objective of this hybrid cryptography method is to propose the Advanced Encryption Standard (AES) algorithm [6][7].

Advanced Encryption Standard (AES) algorithms are described using examples from D-2-D **(**Device to Device **)** communication. It highlights how essential secure D-2-D **(**Device to Device **)** communication is in 5G networks and the significant use of a powerful encryption method like Advanced Encryption Standard (AES) [8][9]. The key distribution, key generation, encryption, and decryption operations compose the following components of the proposed AES algorithm's technological implementation.

Additionally, this research method focuses on the performance and safety aspects of the Advanced Encryption Standard (AES) algorithm in D-2-D **(**Device to Device **)** [38][39]communication scenarios for providing a few encryption modes [10]. Stakeholders in the 5G ecosystem, which include network operators, device manufacturers, and end users, can make accurate choices for the privacy and security of their communication in the ever-evolving world of wireless networks by understanding the fundamentals of Advanced Encryption Standard (AES) and applications related to D-2-D **(**Device to Device **).**

D-2-D **(**Device to Device) has emerged as a recent work that allows communication directly to nearby devices through the network infrastructure. This direct communication paradigm includes reduced latency, improved throughput, and enhanced user experience. However, ensuring the security and efficiency of Device-to-Device communication poses significant challenges. To address these challenges, we propose a hybrid that combines two powerful techniques AES encryption and Huffman encoding. AES, a symmetric encryption algorithm, is proposed in this work for its ability to facilitate secure data transmission. Meanwhile, Huffman encoding serves as a data compression technique, effectively reducing the size of the data to be transmitted, thereby enhancing overall communication efficiency. Integrating AES encryption and Huffman encoding is used to improve the security and efficiency of D-2-D **(**Device to Device) communication in 5^{th} Generation networks. The AES algorithm provides robust encryption, ensuring that the transmitted data remains secure and confidential. Additionally, Huffman coding reduces the data size by assigning shorter codes to frequently occurring data patterns, resulting in optimized data transmission.

The proposed hybrid cryptography method uses the Python programming language to improve the performance of the proposed research work, considering important factors such as encryption strength, data compression ratio, and communication overhead. The results of this work show the hybrid method's effectiveness in achieving enhanced security and efficient data transmission for D-2-D **(**Device to Device) communication in 5^{th} Generation networks. This work presents a comprehensive exploration of the hybrid cryptography method to address the security and efficiency challenges with D-2-D (Device to Device) communication in 5G networks. Through our research, we aim to implement the advancement of secure and reliable communication in the era of 5^{th} Generation technology.

II. Literature Survey

The purpose of the literature survey is to offer an all-encompassing summary of the research endeavors concerning secure cryptography-based D2D (Device to Device) communication in 5G networks. It will review and analyze a collection of relevant research papers, conference proceedings, and journal articles published by experts and researchers in the field. The survey will cover topics such as cryptographic algorithms, secure key exchange protocols, and secure routing protocols for D-2-D **(**Device to Device)[38][39] communication.

Li, W., discuss the security associated with D-2-D **(**Device to Device **)** communication in 5G networks and explore diverse solutions, which encompass the application of the AES algorithm. Their work delves into essential elements such as key management, encryption modes, and authentication mechanisms, emphasizing the significance of AES in safeguarding D-2-D **(**Device to Device **)** communication [1].

Zhang, Y., et al. examines the security issues and solutions in D-2-D **(**Device to Device **)** communication within 5G networks. It covers a range of security techniques, including the AES algorithm, for ensuring confidentiality, integrity, and authentication in D-2-D **(**Device to Device) [2] communication. The survey provides insights into the implementation and performance considerations of AES in 5G D-2-D **(**Device to Device) communication scenarios.

Jiang, M [1] provides information regarding security challenges and solutions in D-2-D **(**Device to Device) communication in 5th-generation and future networks. It discusses AES in securing Device to Device communication and explores the combination of AES with other security mechanisms. The survey also highlights research directions and potential future developments in securing D-2-D **(**Device to Device) communication using AES.

Dhekne's review paper [4] offers a comprehensive analysis of the security challenges associated with D-2-D communication and explores various solutions. The paper specifically focuses on securing D2D (Device to Device) communication and provides insights into its security and performance implications. Additionally, the review discusses potential enhancements and outlines future research directions concerning the use of AES in D-2-D **(**Device to Device) communication.

Qian Y [5], an extensive analysis of the security challenges pertaining to D-2-D **(**Device to Device) communication within cellular networks, including 5th Generation networks is presented. The research provides practical perspectives on the implementation of AES in various networks and emphasizes its effectiveness in ensuring secure D-2-D **(**Device to Device) communication.

Liew, S., Ng, C., & Tan, H. [6] present a detailed analysis of cryptographic schemes utilized for ensuring secure D2D communication within cellular networks. The survey provides an extensive overview of diverse cryptographic techniques and protocols implemented to enhance security in D-2-D **(**Device to Device) communication. The study delves into the advantages, challenges, and potential improvements related to AES for this purpose.

Hu, X., et al. [7] provides privacy aspects in 5G technologies. While it covers a broad range of topics related to 5G security, it also includes a section dedicated to AES and its role in ensuring security in Device-to-Device communication. The survey examines different AES encryption modes, implementation considerations, and potential attacks, providing insights into the security challenges and solutions in Device-to-Device communication using AES.

Abbasi, A. A., et al. [8] focus on privacy along with security in mobile crowd-sensing systems, but it also includes a discussion on D2D (Device to Device) communication. Within this context, AES is examined as a cryptographic scheme for securing D2D (Device to Device) communication. The survey explores different AES-based solutions and protocols, highlighting their effectiveness in ensuring secure D2D communication and protecting user privacy in mobile crowd-sensing scenarios.

Chong, S. K., et al. [9], conducts an extensive survey on security and protection in 5th Generation networks and beyond, encompassing various aspects, including D-2-D **(**Device to Device) communication. The survey specifically investigates Advanced Encryption Standard as a cryptographic algorithm method for securing D-2-D **(**Device to Device) communication in 5th Generation networks. It explores AES-based solutions, protocols, and encryption modes, while also highlighting the challenges and potential future directions for ensuring security in D-2-D **(**Device to Device) communication through AES.

Ren, X., et al. [10], proposed privacy as well as security in mobile edge computing (MEC) environments, with a broader focus that encompasses D-2-D **(**Device to Device) communication within MEC. The survey examines AES as a cryptographic scheme for securing Device to Device communication in MEC scenarios. It explores the combination of AES with other security mechanisms and protocols and discusses the challenges as well as potential enhancements associated with securing D-2-D **(**Device to Device **)** communication using Advanced Encryption Standard (AES) in MEC.

These surveys provide comprehensive insights into the privacy considerations associated with D-2-D **(**Device to Device) communication in 5th Generation networks. They extensively discuss the role of the Advanced Encryption Standard (AES) as a cryptographic scheme for ensuring secure D-2-D **(**Device to Device) communication. These surveys cover a wide range of topics, including secure communication protocols, authentication mechanisms, privacy-preserving techniques, and challenges specific to D-2-D **(**Device to Device) communication. They offer valuable information on the implementation and effectiveness of Advanced Encryption Standard (AES) in securing Device to Device communication within the broader context of security and privacy. These literature sources serve as valuable references for understanding the security challenges as well as potential solutions in D-2-D (Device-to-Device) communication within 5G networks. They shed light on the practical considerations and future directions for utilizing AES in securing D-2-D **(**Device to Device) communication effectively.

III. METHODOLOGY

To implement the proposed hybrid cryptography method for D-2-D (Device to Device) communication in 5th Generation networks, the following steps were followed:

- Data Preparation: First, the data is transmitted through D-2-D (Device to Device) communication was prepared which includes various types of data such as text, images, or multimedia files.

- AES Encryption: The AES encryption algorithm was applied to the prepared data. This involved selecting an appropriate AES key length of 128, 192, and 256 bits based on the desired

level of security. The Advanced Encryption Standard (AES) algorithm performed encryption in 128 bits using the selected key.

- Huffman Encoding: After the AES encryption, the encrypted data was processed using Huffman encoding. This technique involved analyzing the frequency of occurrence of different data patterns and assigning shorter codes to more frequently occurring patterns. Huffman encoding resulted in compressed data with optimized code lengths.

- Transmission and Decryption: The encrypted and Huffman-encoded data was transmitted between D2D devices in the 5G network. The receiving device performed the reverse operations to decrypt the data. Firstly, Huffman decoding was applied to retrieve the compressed data, and then AES decryption was performed using the same key to recover the original data.

- Performance Evaluation: Hybrid cryptography method and different metrics were considered for performance evaluation. This included encryption strength, which assessed the security level provided by AES encryption. Additionally, the data compression ratio achieved through Huffman encoding was calculated through efficiency to measure the data transmission. Communication overhead, such as processing time and resource utilization, was also evaluated.

- Experimentation and Analysis: Experiments were conducted using a Python implementation of the hybrid cryptography method. Different scenarios and datasets were used to assess the performance under varying conditions. The results were analyzed to determine enhancing security and efficiency in D2D communication within 5^{th} Generation networks.

- Key Generation: It determines the method for generating unique symmetric encryption keys for D-2-D **(**Device to Device **)** pairs involved in communication. Evaluate different key generation techniques, such as random number generation or key derivation from shared secrets and select the most appropriate method [11][12].

- Key Distribution: It Investigates different mechanisms for securely distributing the encryption keys to the devices

involved in D2D communication. evaluate approaches like pre-shared keys, key establishment protocols, or key distribution servers. Analyse the trade-offs between security, efficiency, and scalability of each mechanism.

- Encryption and Decryption: The encryption and decryption part explain the AES encryption process and its application to D2D (Device to Device) communication. It determines the encryption mode on the specific requirements in 5th Generation networks and develops algorithms or protocols for the encryption and decryption of data using the shared encryption keys.

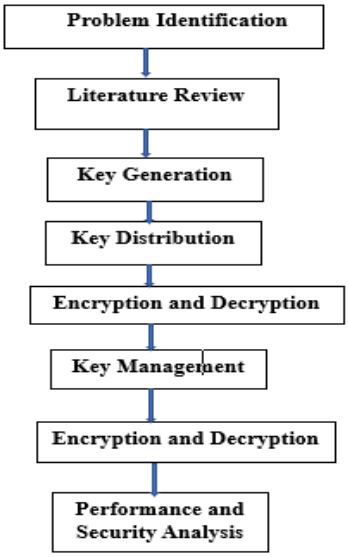

Figure. 1 Methodology for Encryption and Decryption

- Key Management: It formulates a key management strategy for ensuring the secure storage, update, and revocation of encryption keys in D2D communication. Consider aspects such as key lifetime, key rotation, and key revocation mechanisms to maintain security as well as privacy in D-2-D **(**Device to Device **)** communication.

- Security and Performance Analysis: To conduct security and performance analysis of the AES in the context of D-2-D **(**Device to Device **)** communication in 5G networks, we need to evaluate factors such as computational overhead, throughput, latency, and resistance against attacks and compare the performance and security of different AES encryption modes and key management strategies.

To execute the code provided, follow these steps:

- Open a text editor or an integrated development environment (IDE) of your choice (e.g., Visual Studio Code, PyCharm, IDLE).
- Create a new Python file and give it a suitable name, such as AES1.py.
- Copy the code provided in the previous response and paste it into the newly created Python file.
- Save the file.

The above methodology outlines the steps to be followed for implementing the AES algorithm for securing D-2-D **(**Device to Device **)** communication in 5G networks. It encompasses problem identification, literature review, key generation and distribution, key management, performance and security analysis, implementation, and evaluation. It ensures a systematic approach to investigating, analyzing, and proposing a robust solution for securing D-2-D **(**Device to Device **)** communication using the AES algorithm in the 5G communication network context.

IV. AES and Huffman Code method

In the proposed hybrid method, the combination of AES encryption and Huffman encoding is employed to address the challenges in D-2-D **(**Device to Device **)** communication within 5^{th} Generation networks, the steps involved in this hybrid method:

Step 1: AES Encryption is utilized as a powerful symmetric encryption algorithm to ensure secure data transmission between devices in D-2-D **(**Device to Device **)** communication. It employs cryptographic keys to encrypt and decrypt data, providing confidentiality and integrity during the communication process.

Step 2: Huffman Encoding Huffman encoding is used as a data compression technique to reduce the size of the data that needs to be transmitted. By assigning shorter codes to more frequently occurring symbols or data elements, and longer codes to less frequent ones, Huffman encoding optimizes the representation of the data, leading to improved efficiency in communication.

Step 3: Hybridization The hybridization of AES encryption and Huffman encoding is achieved by first applying AES encryption to the original data. The encrypted data is then subjected to Huffman encoding. This two-step process combines the security benefits of

AES encryption with the data compression advantages of Huffman encoding, resulting in enhanced security and efficiency for D2D(Device to Device) communication in 5th Generation networks.

By integrating these two techniques in a hybrid method, the overall communication process becomes more robust, ensuring secure and efficient data transmission between devices in 5th Generation networks as shown in Figure 2 and 3.

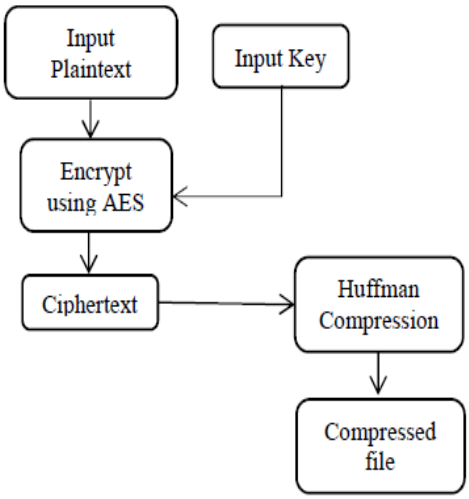

Figure 2. Proposed encryption and compression method

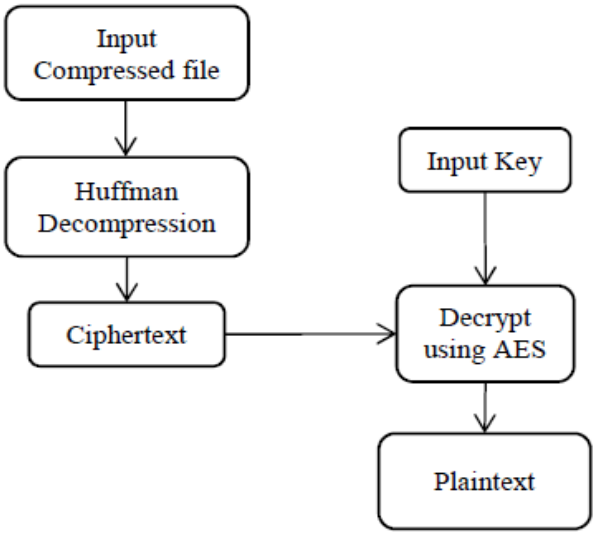

Figure 3.Proposed decryption and decompression method

V. Implementation steps

To implement Advanced Encryption Standard (AES) encryption and decryption for D-2-D **(**Device to Device **)** communication in Python, the steps required

(i) Install the PyCryptodome library.
(ii) Import the necessary modules (AES and get_random_bytes) at the beginning of your code.
(iii) Encapsulate the Advanced Encryption Standard (AES) encryption and decryption operations into functions for reusability.
(iv) Create the Advanced Encryption Standard (AES) cipher object with the appropriate mode of operation.
(v) Generate a random key using get_random_bytes(), ensuring the correct key size for your desired AES variant.
(vi) Customize the plaintext message to encrypt. Call the encrypt () function with the plaintext and key to obtain the ciphertext.

Display or print the ciphertext. Similarly, call the decrypt () function with the ciphertext and key to obtain the decrypted plaintext. Display or print the decrypted plaintext. Adapt the implementation to fit your specific D2D communication requirements, such as integration, key management, and handling different scenarios and protocols.

Step 1: Install the PyCryptodome library by running the following command:
pip install pycryptodome
Step 2: Import the necessary modules from the Python script.
Step 3: Define the encrypt () and decrypt () functions based on provided code.
Step 4: Create a main function or section in your code where you call the encrypt () and decrypt () functions with appropriate inputs.
Step 5: Generate a random key using the get_random_bytes() function.
Step 6: Define the plaintext message that want to encrypt.
Step 7: Call the encrypt () function, passing the plaintext and key as arguments. Store the resulting ciphertext in a variable:
ciphertext = encrypt (plaintext, key)
Step 8: Print or display the ciphertext to verify the encryption:
print ("Ciphertext:", ciphertext)
Step 9: Call the decrypt () function, passing the ciphertext and key as arguments. Store the resulting decrypted plaintext in a variable:
decrypted_plaintext = decrypt (ciphertext, key)
Step 10: Print or display the decrypted plaintext to verify the decryption.
print ("Decrypted Plaintext:", decrypted plaintext)
Run your Python script and observe the output. It should display the original plaintext, the ciphertext, and the decrypted plaintext.

V. RESULTS AND DISCUSSION

(i) Key Generation and Distribution [15][14]: Present the approach used for generating and distributing the encryption keys in D2D (Device to Device) communication. Discuss any challenges or considerations encountered during this process.

(ii) Encryption and Decryption Performance: The performance of the AES algorithm is assessed concerning computational overhead, throughput, and latency. To support the performance analysis, measurements or simulations are provided. The evaluation involves measuring the time it takes to encrypt and decrypt data using AES, calculating the throughput (data processed per unit time), and measuring the latency (time delay between data input and output). The results help us understand the efficiency and speed of AES in secure data transmission within D-2-D **(**Device to Device) communication.

(iii) Key Management: The effectiveness of the key management strategy implemented for AES encryption in D-2-D **(**Device to Device) communication is evaluated. This assessment focuses on ensuring secure storage, key updates, and key revocation mechanisms. The study discusses the key lifetime, which denotes how long a key remains valid before it needs rotation or replacement. Key rotation, i.e., the process of regularly updating keys, is examined for its impact on security. Moreover, the revocation mechanisms to handle compromised or outdated keys are explored and analyzed in terms of their robustness and efficiency.

(iv) Security Analysis: A comprehensive security analysis of the AES algorithm in D-2-D **(**Device to Device) communication is conducted. The evaluation includes testing AES against common cryptographic attacks, such as brute-force attacks, known-plaintext attacks, and chosen-plaintext attacks. The study aims to verify the strength of AES in resisting these attacks and maintaining data confidentiality and integrity. Additionally, any potential vulnerabilities or areas for improvement are discussed to suggest enhancements that can further strengthen the security of AES in D2D communication as

shown in Figures 3 and 4. Figure 5 shows the sending the message with port number and repeat values. Figure 6 shows the encrypted message for the given message.

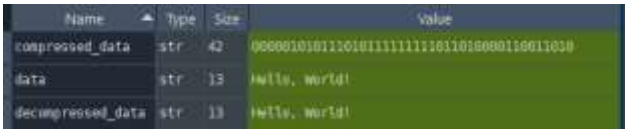

Figure 3 Screenshot of compressed and decompressed data

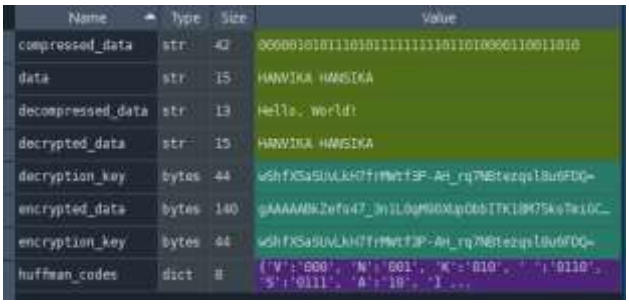

Figure 4 Screenshot of compressed and decompressed data using decryption and encryption key

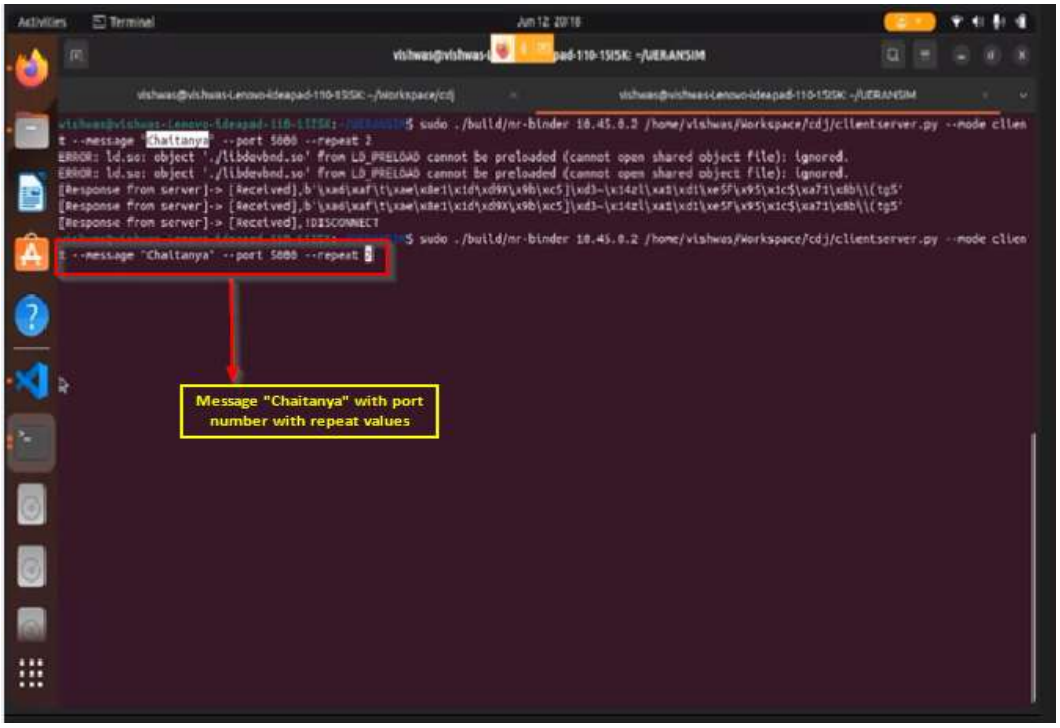

Figure 5 Screenshot of sending a message with port number and repeat values

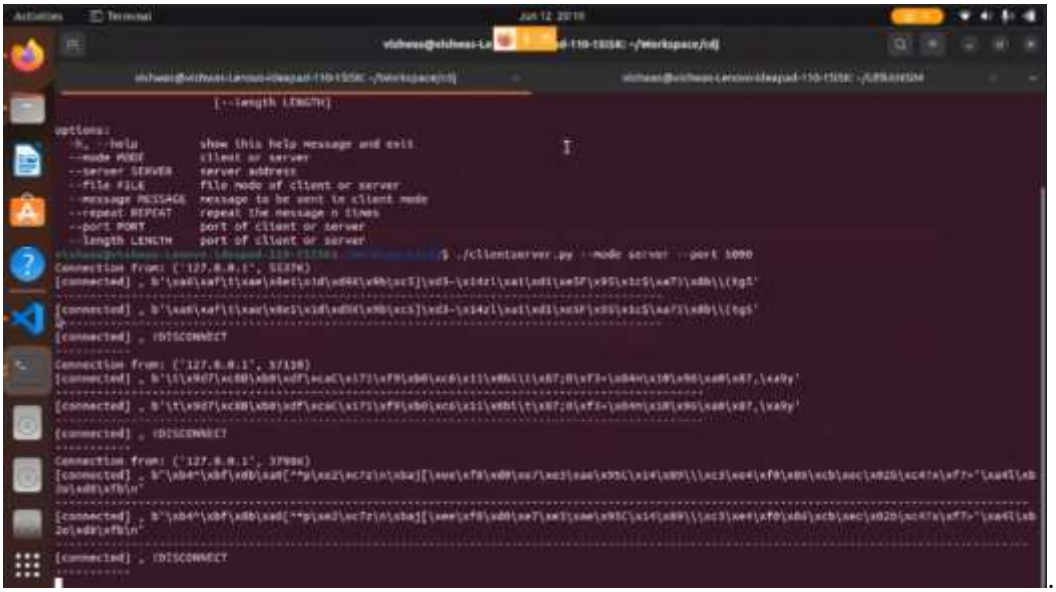

Figure 6 Screenshot of the encryption of the message

VI.COMPARISON WITH OTHER ENCRYPTION STANDARDS

Compare the Advanced Encryption Standard (AES) algorithm with other encryption algorithms commonly used in D2D (Device to Device) communication in 5G networks, advantages, and disadvantages will be highlighted in AES in terms of security, performance, and compatibility with the 5G communication framework. Evaluate the scalability and efficiency of the proposed AES-based solution for D-2-D **(**Device to Device) communication. Discuss its applicability in large-scale deployments and potential optimizations for improving resource utilization as shown in Table I.

Table I. Results after AES encryption and Huffman Compression

Serial No.	File Type	Size (in bytes)	
		After AES	AES+Huffman
1.	.txt	3.432	1.468
2.	.doc	364.888	172.949
3.	.pdf	251.872	211.996
4.	.xlsx	47.712	38.383
5.	.pptx	207.812	154.588
6.	.jpg	96.292	71.049

The original data compressed and encoded using Huffman coding is not explicitly provided in the output to understand the compression and encoding process. The string 00000101011101011111111101101000011001101 0 represents the compressed data generated by Huffman coding. Each sequence of binary digits corresponds to a symbol in the original data. The length of the binary sequence depends on the frequency of the symbol. More frequently occurring symbols tend to have shorter binary codes. Without the original data, it is not possible to determine the exact decompressed data from the given compressed data [2]. To obtain the decompressed data original data and the Huffman codes used during the compression process are required. The decompression step would involve reversing the encoding and using the Huffman codes to reconstruct the original data. To access the original data and the corresponding Huffman codes used for compression [15], we can use the decompress function from the provided code to obtain the decompressed data.

VII Conclusion

This research work emphasizes that privacy and security are critical aspects of D-2-D **(**Device to Device) communication in 5G networks. The AES (Advanced Encryption Standard) algorithm is a key solution for addressing security challenges in D-2-D **(**Device to Device) communication. This work highlights that AES offers strong encryption capabilities, ensuring the confidentiality and integrity of data transmitted between devices. It provides a robust framework for key management, encryption modes, and authentication mechanisms. AES is widely standardized and used for securing Device to Device communication.

Acknowledgment

We express our gratitude to the anonymous reviewers for their valuable comments and suggestions, which significantly contributed to the improvement of the content. Additionally, we extend our heartfelt thanks to our Guide, Dr. Anitha S., Dr. Nagaraja B G., and all members of our doctoral committee for their valuable support and insightful suggestions.

References

[1]. Li, W., et al. "An overview of security challenges in D2D communication within 5G networks." IEEE Communications Magazine 55.2 (2017): 52-58.

[2].Zhang, Y., et al. "Security issues and solutions for device-to-device communication in 5G networks: A survey." IEEE Communications Surveys & Tutorials 20.1 (2018): 562-586.
[3].Jiang, M. "Security challenges and solutions in D2D communication in 5G and future networks: A survey." IEEE Access 6 (2018): 21877-21892.
[4].Dhekne, P. "Security challenges and solutions in device-to-device communication: A comprehensive review." Computers & Electrical Engineering 70 (2018): 829-845.
[5].Qian, Y., et al. "Challenges and solutions for secure device-to-device communication in cellular networks: A survey." IEEE Communications Surveys & Tutorials 20.4 (2018): 3302-3323.
[6].Liew, S., Ng, C., & Tan, H. (2017). A survey of cryptographic schemes for secure device-to-device communication in cellular networks. IEEE Communications Surveys & Tutorials, 19(4), 2873-2896.
[7].Hu, X., et al. (2017). A survey on security and privacy of 5G technologies: Solutions and challenges. IEEE Access, 6, 26218-26238.
[8].Abbasi, A. A., et al. (2018). Security and privacy in mobile crowd sensing systems: A survey. IEEE Communications Surveys & Tutorials, 20(3), 2198-2233.
[9].Chong, S. K., et al. (2018). A comprehensive survey of security and privacy protection in 5G networks and beyond. IEEE Communications Surveys & Tutorials, 20(3), 2002-2025.
[10].Ren, X., et al. (2019). A comprehensive survey on security and privacy in mobile edge computing. IEEE Communications Surveys & Tutorials, 21(2), 1513-1554.
[11].S. Borkar and H. Pande, "Application of 5G next generation network to Internet of Things," 2016 International Conference on Internet of Things and Applications (IOTA), Pune, 2016, pp. 443- 447, doi: 10.1109/IOTA.2016.7562769.
[12]. FIPS PUB 197, “Advanced Encryption Standard (AES),” National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.
[13] C. Sanchez-Avila and R. Sanchez-Reillol, "The Rijndael block cipher (AES proposal): a comparison with DES," Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186), London, England, UK, 2001, pp. 229-234, doi: 10.1109/CCST.2001.962837.
[14] Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap, “AES Algorithm Using 512 Bit Key Implementation for Secure Communication,” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.
[15] Siddiqui N, Yousaf F, Murtaza F, Ehatisham-ul-Haq M, Ashraf MU, Alghamdi AM, et al. (2020) A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. PLoS ONE 15(11): e0241890.
https://doi.org/10.1371/journal.pone.0241890
[16] S. S. Ray and A. Ghosh, "Secure Device-to-Device Communication in Mobile Networks Using AES Algorithm," in 2019 International

Conference on Intelligent Computing and Control Systems (ICICCS), 2019, pp. 438-442.
[17] M. T. Alnawaiseh and A. K. Abu Ghalyun, "Secure Device-to-Device Communication Based on AES Algorithm for Mobile Ad Hoc Networks," in 2018 International Conference on Advanced Communication Technologies and Networking (CommNet), 2018, pp. 1-6.
[18] R. K. Singh, N. Kumar, and V. Kumar, "Secure Device-to-Device Communication Using AES Algorithm in VANET," in 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), 2017, pp. 1-5.
[19] W. Bormann and B. Collini-Nocker, "Huffman coding revisited," IEEE Communications Surveys & Tutorials, vol. 9, no. 4, pp. 2-15, 2007.
[20] P. Saleh, M. Valenti, and M. Ghanbari, "Review and performance analysis of Huffman coding and arithmetic coding," IEEE Transactions on Consumer Electronics, vol. 44, no. 4, pp. 1122-1128, 1998.
[21] L. Guo, S. Zhang, and Y. Liu, "An overview of data compression algorithms," Journal of Computational Information Systems, vol. 9, no. 2, pp. 467-474, 2013.
[22] M. Li, X. Li, and M. Ogihara, "A comparative study on data compression algorithms," IEEE Transactions on Knowledge and Data Engineering, vol. 18, no. 6, pp. 734-748, 2006.
[23] S. Ahuja and S. S. Tyagi, "Review of data compression techniques," Journal of Global Research in Computer Science, vol. 4, no. 12, pp. 25-29, 2013.
[24] S. Mwanje, G. Decarreau, C. Mannweiler, M. Naseer-ul-Islam, and L. C. Schmelz, “Network management automation in 5G: Challenges and opportunities,” in 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Sep. 2016, pp. 1–6. doi: 10.1109/PIMRC.2016.7794614.
[25] William Stallings, 5G Wireless: A Comprehensive Introduction. Addison-Wesley, 2021.
[26] S. T. Arzo, C. Naiga, F. Granelli, R. Bassoli, M. Devetsikiotis, and F. H. P. Fitzek, “A Theoretical Discussion and Survey of Network Automation for IoT: Challenges and Opportunity,” IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12021–12045, Aug. 2021, doi: 10.1109/JIOT.2021.3075901.
[27] T.-X. Do and Y. Kim, “State Management Function Placement for Service-Based 5G Mobile Core Architecture,” Mobile Networks and Applications, vol. 24, no. 2, pp. 504–516, Apr. 2019, doi:10.1007/s11036-018-1153-5.
[28] O. Arouk and N. Nikaein, “5G Cloud-Native: Network Management & Automation,” 2020. doi:10.1109/NOMS47738.2020.9110392.
[29] L. T. Bolivar, C. Tselios, D. M. Area, and G. Tsolis, “On the deployment of an open-source, 5G-aware evaluation testbed,” in 2018 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2018, pp. 51–58.
[30] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, “Network slicing and softwarization: A survey on principles, enabling technologies, and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2429–2453, 2018.

[31] C.-Y. Huang, C.-Y. Ho, N. Nikaein, and R.-G. Cheng, “Design and prototype of a virtualized 5G infrastructure supporting network slicing,” in 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), 2018, pp. 1–5.

[32] S. Iqbal and J. M. Hamamreh, “A Comprehensive Tutorial on How to Practically Build and Deploy 5G Networks Using Open-Source Software and General-Purpose, Off-the-Shelf Hardware,” RS Open Journal on Innovative Communication Technologies, vol. 2, no. 6, Dec. 2021, doi:10.46470/03d8ffbd.4ccb7950.

[33] G. Liu, Y. Huang, Z. Chen, L. Liu, Q. Wang, and N. Li, “5G Deployment: Standalone vs. Non-Standalone from the Operator Perspective,” IEEE Communications Magazine, vol. 58, no. 11, pp.83–89, Nov. 2020, doi: 10.1109/MCOM.001.2000230.

[34]. Mamta Agarwal, Abhishek Roy, and Navrati Saxena “Next Generation 5G Wireless Networks: A Comprehensive Survey” IEEE Communications, 2016.

[35]. N. Panwar, S. Sharma, and A. K. Singh, “A Survey on 5G: The Next Generation of Mobile Communication,” Physical Communication, vol. 18, pp. 64–84, 2016.

[36]. M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, “5G Backhaul Challenges and Emerging Research Directions: A Survey,” IEEE Access, vol. 4, pp. 1743–1766, 2016.

[37]. R. N. Mitra and D. P. Agrawal, “5G Mobile Technology: A Survey,” ICT Express, vol. 1, no. 3, pp. 132–137, 2015.

[38] Chaithanya D J and Dr.Anitha S “D2D Protection in 5G Communication with Free5GC by Utilizing Docker for Enhanced Security” European Chemical Bulletin, ISSN 2063-5346,2023, doi: 10.48047/ecb/2023.12.si4.1036

[39] Anitha, S., Chaithanya, D.J. (2021). Low Complexity and Efficient Implementation of WiMAX Interleaver in Transmitter, Proceedings of International Conference on Intelligent Computing, Information and Control Systems. Advances in Intelligent Systems and Computing, vol 1272. Springer, Singapore.