SVU-International Journal of Engineering Sciences and Applications (2025) 6(1): 152-159
Print ISSN 2785-9967 | Online ISSN 2735-4571
DOI 10.21608/svusrc.2025.329506.1243

Multi-Layer Security Framework for Secure Communication in Internet of Vehicles Networks

Mahmoud Elomda[1, □], Ahmed A. Ibrahim[2], and Mahmoud Abdelaziz[3]

Abstract In the ever-evolving landscape of data security, the need for robust encryption mechanisms remains paramount. This paper introduces a novel concatenated encryption system that leverages the strengths of both the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). The proposed system sequentially applies DES and AES to plaintext data, combining the legacy robustness of DES with the modern security features of AES. This dual-layer encryption aims to enhance overall security, particularly against emerging cryptanalytic techniques. The concatenated DES-AES encryption system is evaluated for its security efficacy, computational performance, and practical applicability. The security analysis demonstrates that the dual encryption approach provides increased resistance to brute-force attacks and sophisticated cryptanalysis by leveraging the distinct encryption strengths of DES and AES. Additionally, the system benefits from AES's enhanced security features while utilizing DES's well-understood cryptographic foundation. However, the proposed system is not without its drawbacks. The primary disadvantage is the increased computational overhead due to the sequential application of two encryption algorithms. This results in a higher processing time compared to using a single encryption standard. Furthermore, while the concatenated approach increases security, it does not address the inherent vulnerabilities of DES, such as its susceptibility to brute-force attacks when used alone. The system's performance impact and complexity in implementation must be carefully considered in its deployment. The FPGA implementation will be presented in this paper to validate the concept of this paper.

Keywords: Cryptography; FPGA; IOV; Mobile; OFDM.

Received: 29 October 2024/ Accepted: 24 January 2025

□Corresponding Author: Mahmoud Elomda, el3omda999@hotmail.com
Ahmed A. Ibrahim, ahmedabdel_monem@mu.edu.eg,
Mahmoud Abdelaziz, mkaremm@mtc.edu.eg
1., 2. Electrical Engineering Department, Faculty of Engineering, Minia University,Egypt
3. Avionics Department, Military Technical College ,Egypt

1 Introduction

Numerous standardization organizations have largely finalized discussions and experimental validation of 5G communication technology, culminating in the termination of Third Generation Partnership Project (3GPP) R15 [1]. The experimental commercial network is currently undergoing actual testing, signaling that the mobile internet is on the brink of entering the 5G era. The 5G network facilitates seamless integration of 2G, 3G, 4G, WiFi, and other access technologies, offering speeds exceeding 10Gb/s, low latency, high reliability, ultra-high user capacity, and support for high mobility, among other features. Additionally, 5G not only supports a wider range of application scenarios in the mobile internet such as ultra-high definition visual communication, multimedia interaction, mobile industrial automation, and vehicle interconnectivity but is also extensively utilized in the IoT, encompassing mobile healthcare, smart homes, industrial control, automotive networking, and environmental monitoring. Hundreds of billions of devices connect to the 5G network, facilitating the "Internet of Everything." Compared to 3G and 4G, the upcoming 5G network will feature diverse terminals and a vast number of nodes, ultra-high-density node deployment, coexistence of various wireless network technologies and security measures, end-to-end direct communication, and the integration of new techniques like Vehicle-to-Everything (V2X).These innovations will present several new security challenges for 5G networks.

3GPP organizations have undertaken preliminary research and established several standards concerning 5G security. For instance, 3GPP TS 33.501 has created a new security framework for 5G that encompasses the security features and mechanisms of 5G systems and core networks, as well as their operation within 5G core networks and new radio access networks. Additionally, 3GPP TR 33.811 has focused on security research related to network slice management, proposing features, identifying security threats, outlining security requirements, and offering solutions for 5G network slice management [2]. Meanwhile, 3GPP TR 33.841 has examined the security threats and impacts on User Equipment (UE), NR Node B (gNB), and core network entities regarding symmetric and asymmetric encryption algorithms in the post-quantum era. It also explored the use of a 256-bit key length encryption algorithm in 5G, covering key derivation, Authentication and Key Agreement (AKA) key generation, key integrity protection, key distribution, key refresh, and key size negotiation to ensure the security of 5G system in the future [3].

5G-V2X presents numerous advantages, including a significantly larger coverage area, pre-existing infrastructure, deterministic security, QoS guarantees, and enhanced scalability [4],[5]. However, it still faces security and performance challenges, such as a centralized architecture, various authentication types for different scenarios, securing broadcast messages for one-to-many V2X communication, and protecting the privacy of V2X User Equipment (UE) [6],[7][8]. The Internet of Vehicles (IoV) enables seamless connectivity, data exchange, real-time traffic management, and autonomous driving through technologies like OFDM, which improve spectral efficiency and channel capacity, ultimately enhancing bandwidth and reliability.

In the context of 5G telecommunications, the application of this combined encryption strategy can offer substantial benefits. The 5G network architecture, characterized by its high data rates, diverse use cases, and expanded connectivity, demands robust security measures to protect sensitive information and ensure the integrity of communications [9],[10]. The use of AES followed by DES can provide an additional layer of security in this environment, safeguarding data transmissions from potential breaches and cyber-attacks.

The combined use of AES followed by DES represents a sophisticated approach to encryption that leverages the strengths of both cryptographic algorithms to offer enhanced security. AES is renowned for its robust security and efficiency, making it a preferred choice for modern encryption needs. DES, though considered less secure on its own, provides an additional layer of defense when used in conjunction with AES. This layered methodology not only integrates the best features of both algorithms but also introduces a heightened level of complexity that significantly increases the difficulty of unauthorized data decryption. By combining AES and DES, this hybrid encryption approach enhances overall resilience and security, addressing the vulnerabilities inherent in single-algorithm encryption methods.

Furthermore, the integration of this hybrid encryption method can also facilitate compatibility with existing legacy systems. Many telecommunication infrastructures still utilize DES due to its historical significance and compatibility with older systems. By incorporating DES as a secondary layer after AES, the encryption scheme can bridge new and old technologies, offering enhanced security while maintaining interoperability within a heterogeneous network environment.

Overall, the combined use of AES followed by DES provides a robust encryption solution that enhances security and resilience in 5G telecommunications. This approach not only protects data against unauthorized access but also supports compatibility with existing systems, making it a versatile and effective method for securing modern communication networks.

Our contributions in this work are described as follows, emphasizing an overview of IOV network architecture, presenting an enhanced encryption algorithm to provide higher security with low latency.

This paper is organized as follows: section (2) presents the literature review and the preivouse realted work, section (3) explain the applied methodology and the proposed algorithm. Section (4) presents the proposed protocol then the simulation and results are presented in section (5). Finally, the conclusion is explained in section (6).

2 Literature Review

The requirements for achieving higher level of security became necessary for 5G, in this section we present some of applicable encryption algorithm that can be used in 5G to save hardware consumption, in addition to achieving minimum level of security without affecting the reliability of 5G network.

In [11-13] The authors emphasize and categorize the challenges of IOT related to the security. By evaluating existing frameworks and protocols, the authors identify critical areas of vulnerability within IoT systems. These papers propose a set of best practices and technological solutions aimed at enhancing the security of IoT devices and networks, emphasizing the need for robust authentication, encryption, and continuous monitoring mechanisms. In [14] The paper explores the cyber security challenges posed by the Internet of Things (IoT) in the context of emerging quantum computing technologies. It discusses how quantum computers have the potential to break traditional cryptographic schemes, which are widely relied upon to secure IoT devices and communications. The authors identify specific vulnerabilities within IoT ecosystems due to the limited computational resources of many devices, making them particularly susceptible to quantum attacks

In [15] The paper compares encryption methods using the AES (Advanced Encryption Standard) algorithm and Salsa20 algorithm, focusing on improved accuracy by employing noise images as keys in AES. The authors discuss the security benefits and enhancements in encryption fidelity achieved with this approach. They also analyze the efficiency and performance of both algorithms when subjected to various tests, highlighting how noise images contribute to stronger encryption. Overall, the study emphasizes the potential of using unconventional key sources to boost encryption accuracy and security in digital data protection. In [16],[17] The authors presented a customized approach to the Advanced Encryption Standard (AES) for enhancing data security in sensitive networks and applications. It discusses the need for adapting AES to meet specific security requirements and performance constraints in different contexts. In [18] the author presents a novel method for generating highly nonlinear and dynamic AES substitution boxes (S-boxes) using chaos-based rotational matrices. The authors discuss the importance of S-boxes in cryptographic systems, particularly in enhancing the security of the Advanced Encryption Standard (AES). They detail their proposed approach, emphasizing its ability to produce dynamic S-boxes that exhibit strong resistance to various cryptographic attacks. In [19] the author focuses on improving the security of Internet of Things (IoT) devices through a modified version of the Advanced Encryption Standard (AES) algorithm. They propose enhancements to the AES algorithm to better meet the security requirements specific to IoT applications, enhancing both performance and resilience against attacks.

In [20] The paper introduces a double-layer security scheme for images, leveraging aggregated mathematical sequences to enhance the encryption process. The approach integrates two distinct layers of security: the first layer employs a mathematical model that generates sequences for initial image scrambling, while the second layer utilizes a unique algorithm for encrypting the scrambled data. The combination of these two layers aims to secure images from unauthorized access and potential manipulation. Experiments illustrate the effectiveness of the proposed scheme in terms of both encryption strength and resilience against various attacks, such as brute force and statistical analysis. In, [21] The paper explores enhancements to traditional encryption algorithms, specifically the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). It focuses on improving the imperceptibility of data hidden within digital media files using the Least Significant Bit (LSB) method. The authors propose a hybrid approach that combines encryption with steganography, allowing sensitive data to be securely embedded in images without noticeable alterations.

3 Methodology

This paper presnets a new technique of double encryption by concatenating the DES and AES to achieve higher level of security.

In practical terms, the dual-encryption method can be applied to secure various aspects of 5G networks, including user data, control signaling, and management communications. For instance, end-to-end encryption of user data transmitted over 5G networks can be reinforced by first applying AES to encrypt the data and then DES to add an extra layer of protection. This approach is particularly beneficial in safeguarding critical communications against sophisticated attacks and ensuring that sensitive information remains secure even if one layer of encryption is compromised.

The combined use of AES followed by DES offers several benefits. The layered approach provides enhanced security by integrating the strengths of both algorithms, creating a defense that is more difficult for attackers to breach. The complexity of decrypting data encrypted with both AES and DES increases the overall resilience of the encryption scheme, making unauthorized access more challenging. Additionally, this hybrid methodology utilizes established cryptographic standards, benefiting from the robust protection of AES and the additional layer of DES, while maintaining compatibility with legacy systems.

The encryption process consists of AES with 128-bits input and two DES with 64-bits output. AES represents the first stage to encrypt the input 128-bit cipher text while the two DES represent the second stage to encrypt the output from AES after dividing the output from AES into two parts. The output of the two DES is 64-bits cipher text for each DES.

The decyption process consists of two DES decryption algorithm with 64-bits input and AES with 128-bits output. To increase the security level, The output of the two DES undergoes through the second stage (AES) to be decrypted once more. The output of the AES is 128-bits plaintext text.

4 Implementation and Experimental setup

This paper proposes a concatenated DES with AES. In encryption process, the AES is first stage in the encryption process. The AES encrypted data will be divided into two 64 bits. Each 64 bits will be transmitted to its DES branch. Figure 1 shows the encryption schematic diagram of the proposed algorithm. As mentioned before, the output of AES is the input of two DES. The schematic diagram consists of six sub-systems. The frequency down conversion converts frequency from 50 MHz to 12.5 MHz because the input is serial and the data will be transmitted in parallel form of 8-bits to the DES. So the serial-to-parallel block reads the data in serial format using 50-MHz and transmittes the it in parallel form using 12.5-MHz. after converting each serial 8-bits to parallel, the DES and AES blocks perform the encryption process and use 12.5 MHz to receive and transmit. The buffer block stores the encrypted data.

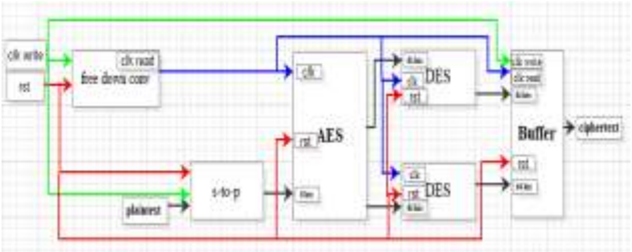

Fig. 1 Encryption schematic Diagram

Figure.2 shows the decryption schematic diagram of the proposed algorithm. the output of DES is 64-bit and the input of AES is 128-bit, so there are two parallel branches of DES. After DES decryption. The output of two DES branches will be transmitted to the AES to perform the second stage of the decryption. To save memory and reduce the hardware consumption as much as possible, the S-box of the AES will be used also in DES stage. AS the AES S-box consists of 16*16 elements and the DES uses 8 S-boxes each one of them is 4*4 elements so the AES will be divided into 8 DES S-box. For more enhancement of the encryption process the order of these S-boxes will not be the same in the two DES branches. The proposed technique enhances the cryptographic processes but consume more hardware and more time to encrypt the data. The decryption process will be mirrored of the encryption process.

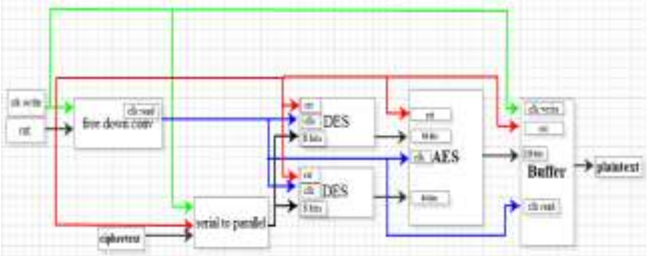

Fig. 2 Decryption schematic Diagram

5 Simulation Results

Four items are required to set up the experimental test: a laptop, the Spartan 3A/3AN FPGA starter kit, a JTAG cable, and a USB to Serial cable. To download the project onto the FPGA kit and to use the ChipScope tool to obtain samples of the data throughout the FPGA paths, the laptop and FPGA kit are connected via JTAG. The UART protocol is used to send and receive the coefficients through a USB to Serial cable.

Figure 3, depicts the experimental setup. The following test configuration is suggested in evaluating the real-time result inside the lab: The Matlab software will convert the image into digital coefficients, and these coefficients will then be transmitted to the FPGA Kit through the USB TO Serial cable using the UART protocol. Using the FPGA, after the encryption and decryption, the data will be transferred to the laptop through the USB TO Serial cable so that the images before and after the encryption can be evaluated.

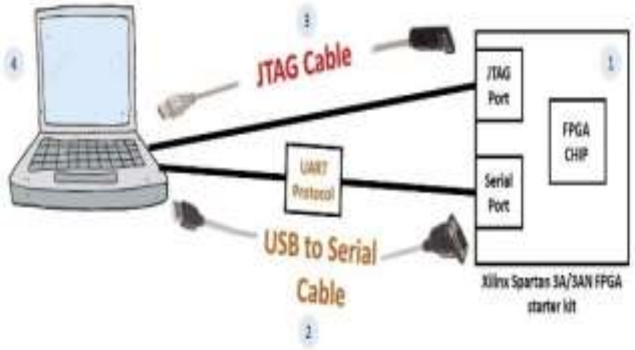

Fig. 3 Lab Test

In this study, the implementation phase utilizes the Kintex 7 Evaluation Board, specifically the "700K-gate XC7K325T-2FFG900C." Custom-crafted VHDL code is developed using the Xilinx ISE 14.7 package, with simulations carried out using the ISim program. The VHDL codeis converted into a schematic representation to streamline the assembly process and simplify debugging tasks.

Figure 4 illustrates the meticulously process of frequency reduction. The simulation employs a clock cycle duration of 20 nanoseconds, corresponding to the initial 50 MHz signal frequency. After the down-conversion process, the clock cycle duration is extended to 160 nanoseconds, which accurately reflects the resulting 6.25 MHz frequency. This transformation confirms that the frequency conversion process effectively achieves the intended output frequency, with the simulation providing a precise representation of both the original and down-converted frequencies.

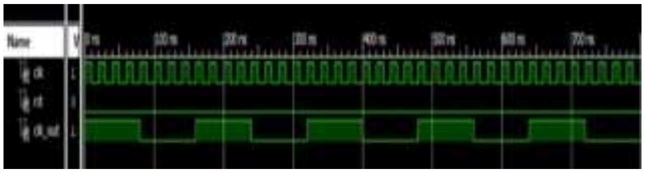

Fig. 4 Frequency Down Conversion

Figure 5 shows simulation result where AES is the first stage followed by DES, the process begins with encrypting a 128-bit plaintext block using AES, resulting in a 128-bit ciphertext. This AES-encrypted output is then divided into two 64-bit blocks. Each 64-bit block is separately encrypted using DES, producing two 64-bit ciphertexts. These DES outputs are then concatenated to form the final 128-bit ciphertext. This sequence of AES followed by DES combines the strengths of both encryption techniques, with AES providing initial encryption and DES adding an additional layer of security.

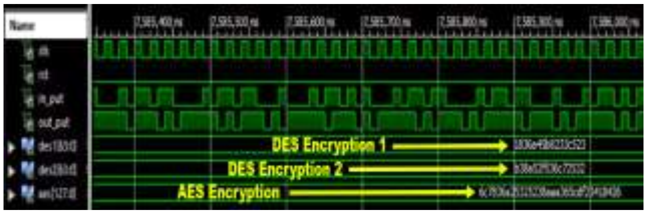

Fig. 5 Encryption Output

Figure 6 shows decryption process where AES is the first stage followed by DES, the sequence is reversed to retrieve the original plaintext. Initially, the final 128-bit ciphertext, which is the result of DES encryption applied after AES, is split into two 64-bit blocks. Each 64-bit block is then decrypted using DES, producing two intermediate 64-bit blocks. These intermediate blocks are then concatenated to reconstruct the 128-bit ciphertext that was originally produced by AES encryption. Finally, this concatenated 128-bit block is decrypted using AES to recover the original plaintext. This decryption process ensures that the multi-layered encryption scheme is properly reversed, utilizing the inverse of each algorithm to accurately retrieve the initial data.

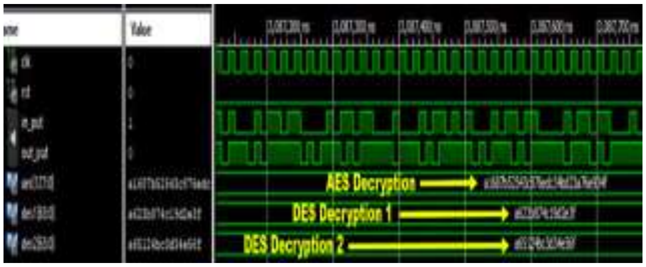

Fig. 6 Decryption Output

In the simulation of AES followed by DES encryption, figure 7 shows the ChipScope analysis, which is crucial for verifying the final 128-bit ciphertext output. ChipScope captures and monitors the entire encryption process, starting from the initial AES encryption of a 128-bit plaintext, through the DES encryption of the resulting two 64-bit blocks, and finally to the concatenation of these blocks into a single 128-bit ciphertext. By providing real-time visibility into each stage, ChipScope ensures that the encryption is performed correctly and that the final 128-bit result meets the expected format and security standards.

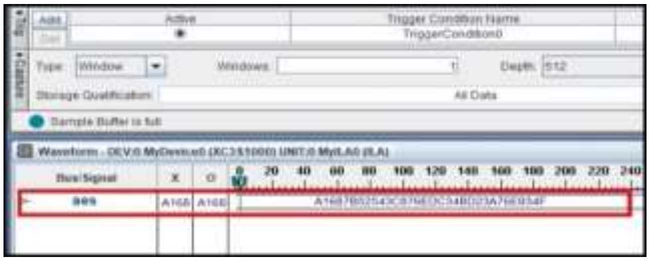

Fig. 7 Encryption Chipscope Analysis

In the decryption process, figure 8 shows the ChipScope, which captures and verifies each step: the 128-bit ciphertext is divided into two 64-bit blocks, decrypted using DES, and then the blocks are reassembled and decrypted with AES to restore the original plaintext. ChipScope ensures the accuracy of these operations by providing real time monitoring and validation.

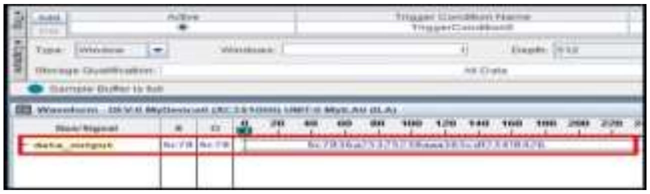

Fig. 8 Decryption Chipscope Analysis

In [22], the author focuses on enhancing data security through the combination of AES and IDEA, emphasizing real-time performance and robust cryptographic guarantees. In contrast, this paper presents an adaptive security system that utilizes DES and AES to address specific security challenges in IOV, particularly for V2X communication. While the proposed system evaluates the performance of the concatenated algorithms in a general context with an emphasis on throughput and resource utilization on FPGA, this paper highlights the importance of dynamic algorithm selection to optimize security without introducing latency, specifically under high mobility conditions.

Table 1 emphasizes a comparison of hardware utilization summary between multi-layer encryprion algorithm and tamper resistance AES.

Table 1 Hardware utilization comparison

Slice logic utilization	Multi-layer		Tamper resistance AES
	TX	RX	
sl reg No.	38222	14782	919
LUTs No.	25389	21078	2582

Moving forward, we will compare our results with those from other study [23], to further evaluate our algorithm's performance and efficiency relative to existing work. This comparison will provide deeper insights into the trade-offs between cryptographic security, hardware utilization, and processing efficiency, allowing us to validate the effectiveness of our multi-layered approach within a broader context.

- **Resistance to Encryption Breaking**: Both systems are robust; however, the proposed algorithm’s use of DES may introduce some vulnerabilities, whereas the tamper-resistant AES offers additional protection through hardware-level tamper resistance, complicating potential attacks.
- **Processing Time:** The proposed algorithm’s multi-stage encryption (AES followed by DES) is more time-intensive compared to the simpler tamper-resistant AES design.
- **Reliability:** Both approaches provide high reliability, though the proposed algorithm, with its multi-layer encryption, may offer enhanced reliability over the tamper-resistant AES, which emphasizes physical tamper resistance.

Table 2 A comparison between the proposed algorithm and a lightweight, tamper-resistant AES implementation on FPGA [23].

Aspect	Tamper resistance AES	Proposed algorithm
Security Effectiveness	Estimated 20-30% improvement in tamper resistance	Estimated 60-70% improvement with concatenated algorithm
Hardware Utilization	Estimated 5-10% area overhead	300-400% increase in FPGA resource utilization (Slices/LUTs)
Throughput	Estimated 200-400 Mbps	Estimated 100-300 Mbps (AES-DES combined)
Latency	Estimated 5-10 microseconds (on board)	Estimated 10-30 microseconds (real-time system)
Simulation and Verification	No detailed simulations provided	Extensive simulations and ChipScope analysis

In conclusion, our proposed algorithm provides enhanced cryptographic security by leveraging a multi-layered AES-DES approach, which increases overall resilience against brute-force attacks and cryptanalysis. This approach contrasts with the tamper-resistant AES implementation, which prioritizes hardware-level defenses to prevent physical tampering. While both systems demonstrate strong security, the proposed algorithm may introduce minor vulnerabilities through the use of DES, but these are balanced by the additional encryption layer.

6 Conclusion

The concatenated DES-AES encryption system offers a promising enhancement in data security by combining the strengths of both DES and AES encryption algorithms. This dual-layer approach provides improved resistance against brute-force attacks and sophisticated cryptanalysis by leveraging the robust foundation of DES alongside the advanced security features of AES. The implementation of the concatenated DES-AES system involves notable hardware consumption due to the sequential application of two encryption algorithms. This design requires additional logic and memory resources to handle the dual encryption stages, which can affect the overall hardware footprint. Efficient design and optimization strategies are crucial to manage these resource demands and ensure the system's practicality for various applications. The sequential processing of DES and AES results in increased computational overhead compared to using a single encryption standard. This leads to higher processing time for both encryption and decryption operations. While the enhanced security provided by the dual-layer approach can be significant, the additional time required for data processing must be weighed against the performance requirements of specific applications. For environments where security is the top priority, this trade-off may be acceptable; however, in scenarios where speed is critical, the increased time consumption could be a notable drawback., while the concatenated DES-AES encryption system enhances security by combining two encryption methods, the increased hardware and time consumption associated with this approach must be carefully considered. Balancing these factors is essential to ensure that the system meets both security and performance needs effectively.

References :

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Rel 15), 3GPP TS 33.501 V15.3.1, Dec. 2018.

[2] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects of 5G network slicing management (Rel 15), 3GPP TR 33.811 V15.0.0, Jun. 2018.

[3] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects, Security aspects; Study on the support of 256-bit algorithms for 5G (Rel 16), 3GPP TR 33.841 V16.0.0, Dec. 2018.

[4] Khan, Muhammad Nawaz, Irshad Khalil, Inam Ullah, Sushil Kumar Singh, Sami Dhahbi, Habib Khan, Abdullah Alwabli, and Mahmoud Ahmad Al-Khasawneh. "Self-adaptive and content-based scheduling for reducing idle listening and overhearing in securing quantum IoT sensors." *Internet of Things* 27 (2024): 101312.

[5] Mangla, Cherry, Shalli Rani, Nawab Muhammad Faseeh Qureshi, and Aman Singh. "Mitigating 5G security challenges for next-gen industry using quantum computing." *Journal of King Saud University-Computer and Information Sciences* 35, no. 6 (2023): 101334.

[6] Naik, Gaurang, Jinshan Liu, and Jung-Min Jerry Park. "Coexistence of wireless technologies in the 5 GHz bands: A survey of existing solutions and a roadmap for future research." IEEE communications surveys & tutorials 20, no. 3 (2018): 1777-1798.

[7] Sayed Ali, Ahmed Zakaria, Aziza I Hussein, and S. Mohamed. "Pico and Femto cells distribution effect on user association performance in 5g heterogeneous networks." Journal of Advanced Engineering Trends 42, no. 1 (2022): 85-93.

[8] Lv, Xiaojiang, Zhi Xiao, Jianguang Fang, Qing Li, Fei Lei, and Guangyong Sun. "On safety design of vehicle for protection of vulnerable road users: A review." Thin-Walled Structures 182 (2023): 109990.

[9] Cao, Jin, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong. "A survey on security aspects for 3GPP 5G networks." IEEE communications surveys & tutorials 22, no. 1 (2019): 170-195.

[10] Sharbaf, Mehrdad S. "IoT driving new business model, and IoT security, privacy, and awareness challenges". 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan." (2022): 1-4.

[11] Lee, In. "The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model." Internet of things 7 (2019): 100078.

[12] Singh, Jaspreet, Gurpreet Singh, and Shradha Negi. "Evaluating security principals and technologies to overcome security threats in IoT world." In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1405-1410. IEEE, 2023.

[13] Nandanwar, Himanshu, and Rahul Katarya. "Deep learning enabled intrusion detection system for Industrial IOT environment." Expert Systems with Applications 249 (2024): 123808.

[14] Althobaiti, Ohood Saud, and Mischa Dohler. "Cybersecurity challenges associated with the internet of things in a post-quantum world." Ieee Access 8 (2020): 157356-157381.

[15] Jashwanth, J., and Kalimuddin Mondal. "Improved Accuracy in File Encryption using Noise Images as Key for AES Algorithm in Comparison with Salsa20 Algorithm." In *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, pp. 1-5. IEEE, 2024.

[16] Mahmoud, Ahmed H., Hanady H. Issa, Nabil H. Shaker, and Khaled A. Shehata. "Customized AES for Securing Data in Sensitive Networks and Applications." In 2022 39th National Radio Science Conference (NRSC), vol. 1, pp. 164-170. IEEE, 2022.

[17] Kaur, Jagpreet, Shweta Lamba, and Preeti Saini. "Advanced encryption standard: attacks and current research trends." In 2021 international conference on advance computing and innovative technologies in engineering (ICACITE), pp. 112-116. IEEE, 2021.

[18] Malik, Muhammad Sarmad Mahmood, Muhammad Asim Ali, Muhammad Asif Khan, Muhammad Ehatisham-Ul-Haq, Syed Nasir Mehmood Shah, Mobashar Rehman, and Waqar Ahmad. "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices." IEEE Access 8 (2020): 35682-35695.

[19] Satyanarayana, P., Narasimhachary Sriramdas, Bondili Madhavi, M. Arun, NV Phani Sai Kumar, and V. Gokula Krishnan. "Enhancement of Security in IoT Using Modified AES Algorithm for IoT Applications." International Conference on Sustainable Communication Networks and Application (ICSCNA), pp. 380-386. IEEE, 2023.

[20] Sari, Christy Atika, Danang Wahyu Utomo, Wellia Shinta Sari, Daurat Sinaga, and Mohamed Doheir. "An Enhancement of DES, AES Based on Imperceptibility Along With LSB." In 2022 International Seminar on Application for Technology of Information and Communication (iSemantic), pp. 150-155. IEEE, 2022.

[21] Elkandoz, Marwa Tarek, Wassim Alexan, and Hisham H. Hussein. "Double-layer image security scheme with aggregated mathematical sequences." In 2019 international conference on advanced communication technologies and networking (CommNet), pp. 1-7. IEEE, 2019.

[22] Hassan, Sara M., and Gihan G. Hamza. "Real-time FPGA implementation of concatenated AES and IDEA cryptography system." Indonesian Journal of Electrical Engineering and Computer Science (ijeecs) 22, no. 1 (2021): 71-82.

[23] Koyanagi, Yui, Tomoaki Ukezono, and Toshinori Sato. "A Light-weight and Tamper-resistant AES Implementation by FPGAs." In *2024 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1-5. IEEE, 2024.