SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Security Enhancement in Iot Based Smart Grid System Using Cryptographic Techniques

P. William[1, 2*], Nilima Patil[3], Kumari Anugya[4], Sandeep Kumar[5], Koyel Roy[6], Tarun Madan Kanade[7]

[1]School of Computer Science and Technology, Karunya Institute of Technology and Sciences (Deemed University), Coimbatore, India. E-mail: william160891@gmail.com
[2]Centre for Research and Consultancy, UNITAR International University, Selangor, Malaysia.
[3]Bharati Vidyapeeth Deemed to be University, Kharghar, Navi Mumbai. E-mail: nilima.patil@bvucoep.edu.in
[4]Symbiosis Law School Hyderabad. E-mail: kumari.anugya@slsh.edu.in
[5]Gopal Narayan Singh University, Sasaram. E-mail: sandeepcnlu@gmail.com
[6]Symbiosis Law School Hyderabad, Symbiosis International (Deemed University), Nandigaon-509217, Hyderabad, Telangana, India. E-mail: koyelroy847@gmail.com
[7]Symbiosis Institute of Operations Management, Symbiosis International (Deemed University), India. E-mail: tarun.kanade@siom.in
*Corresponding Author: P. William E-mail: william160891@gmail.com

Abstract
The phrase "smart grid" denotes a digital electricity distribution system characterized by bidirectional connectivity between the electrical grid and its consumers. Numerous smart grid systems utilize Wireless Sensor Networks (WSNs) as efficient instruments for remote monitoring, fault prediction, and energy management in residential settings. The Internet of Things (IoT) is appealing due to its affordability, versatility, durability, and little energy consumption, with adherence to this low energy consumption being essential. Implementing secure and high-quality services in sensor networks for smart grid applications is challenging. Information and Communication Technology (ICT) constitutes a layer within the smart grid, designed to meet the requirements for grid monitoring, control, and information exchange, hence facilitating efficient grid operation. The smart grid encounters cybersecurity issues through bidirectional communication flows. The diverse smart grid requires protection through multiple cryptographic algorithms based on the availability, privacy, and security of computational resources. A smart grid distribution system may employ a cryptographic encryption and decryption methodology. This study proposed an Enhanced Adaptive TACIT algorithm (IA-TACITA) for secure grid communication. Data samples based on IoT are initially obtained. The collected data is standardized. We employ an optimization approach known as the Enhanced Firefly Optimization approach (EFOA) to expedite data encryption and decryption. The experimental results demonstrate that our proposal achieves greater efficiency than existing solutions.

Keywords: smart grid, IoT, Improved Adaptive TACIT algorithm (IA-TACITA), security, Enhanced Firefly Optimization Algorithm (EFOA), cryptographic algorithm.

1. Introduction

Recent advancements in ICT have become smart grids (SGs) a fundamental component of the IoT infrastructure, enhancing efficiency and reliability in electricity delivery. The SG, a next-generation power grid, incorporates advanced sensors, computing, and communication technologies to enhance electrical network management [1]. SG represents a promising architecture for optimizing energy consumption and transmission due to its integrated information networks, which facilitate bidirectional energy and data flow, promote the extensive integration of renewable energy sources, and empower users to diminish their energy usage. The Internet of Things has rapidly progressed. The Internet of Things (IoT) is facilitating novel methods of interaction between humans and machines through extensive information and communication networks. It denotes a network accessible from any location at any time for the exchange of data regarding any subject. Sensor networks, wireless communication technologies, and IPv6 are the fundamental technical components of the Internet of Things (IoT). The implementation of IoTs is predominantly dependent on wireless sensor or controller networks. The utilization of IoTs spans various domains, including power generation, transmission, substations, distribution, usage, and dispatch, hence rendering IoT security a significant concern within the smart grid. Due to the application-specific nature of IoTs and the unique characteristics of sensor networks in smart grid systems, conventional IoT security techniques cannot be easily implemented in Smart Grid IoTs. Since the inception of the smart grid concept, security has consistently been a paramount concern.

Cryptography is essential while engaging in any unsafe communication, particularly over networks, especially the internet. Cryptography relies significantly on several encryption algorithms that offer different security levels, including a robust key management system. We are likely considered secure if the expense required to compromise an algorithm exceeds the value of the encrypted data [4].

The author [5] concentrated on the Home Area Network (HAN) as it serves as the principal store for sensitive consumer data inside the logical architecture of the smart grid. A security architecture was designed to safeguard the private data of HAN consumers and expedite service delivery. The author [6] presented a cryptographically secure structural architecture for the AES encryption method, enabling rapid throughput and minimal device utilization. The architecture employed the 'S' box approach, yielding a block size and key size of 128 bits.

The study [7] proposed a novel hybrid non-pipelined AES security technique. The "PN sequence generator" is employed to ascertain the values of the S-box for 128-bit key encryption and decryption. A study [8] delineated a strategy for aggregating spatial information, emphasizing "lightweight cryptographic primitives such as one-way hashing function algorithms" and exclusive-OR operations. The study [9] proposed an effective authenticated key agreement method for SGs. This technique facilitates security functionalities including SM privacy and session-key security while functioning inside the widely acknowledged “Canetti-Krawczyk (CK)” adversarial paradigm. A study [10] proposed a lightweight privacy-preserving data aggregation method for smart grids utilizing a “lattice-based homomorphic cryptosystem” to safeguard user privacy and ensure data confidentiality within home area networks.

Article [11] proposed a lightweight methodology via a hybrid cryptography method. The proposed approach encompassed an authentication mechanism alongside a key agreement mechanism. Furthermore, ECC, a symmetric encryption method, a hash function, and a message authentication code were employed to address the numerous security issues inherent in SGs.

This research utilizes a cryptographic method to enhance the security of IoT inside a compact grid framework. This paper's contribution:

1. A dataset based on IoT devices is collected for processing.
2. The dataset undergoes preprocessing through normalization.
3. The Enhanced Firefly Optimization Algorithm (EFOA) is employed for the optimization process.
4. The Improved Adaptive TACIT algorithm (IA-TACITA) is employed to enhance security in IoT devices inside smart grid systems.

The remaining sections of the research are delineated as follows: Part 2, the literature review; Part 3, the study methodology; Part 4, the experimental results; and Part 5, the conclusion.

2. Materials and Methodology

This study examines the methodology employed for augmenting security in IoT-based smart grid systems. The Internet of Things (IoT) is regarded as one of the most efficient applications for implementing Smart Grid technology. The principal security issues and protective measures regarding information requirements in Smart Grid IoTs have been extensively examined. Figure 1 illustrates the methodology overview.

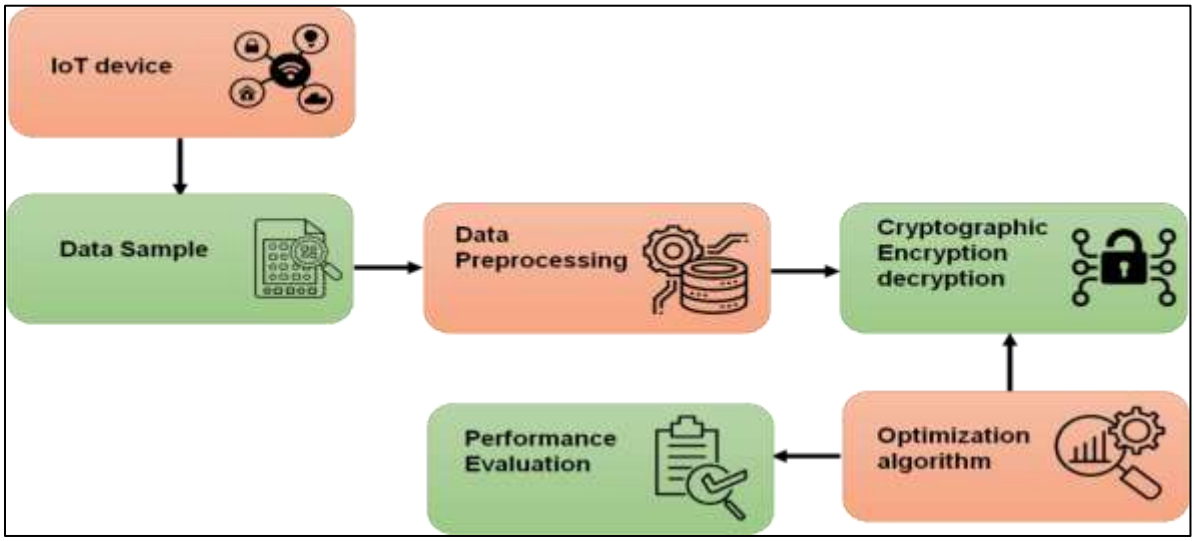

Figure 1: Overview of methodology

A. Dataset description

Two public IoT cloud-edge network datasets, N-BAIOT, are employed to assess our methodology. Given that "IoT-SGAS network traffic," particularly its cloud-edge traffic, closely mimics that of a TCP/IP network, these protocols were employed. The N-BAIOT data collection has 13,113 "normal" entries and 822,763 "threat" entries, encompassing hazards such as "Bashlite and Mirai IoT malware." These risks encompass several activities, including scanning, UDP/TCP flood attacks, and spam dissemination.

B. Data preprocessing

The processing is complicated by the variable quality of the input data Y^y and the unique numeric values associated with each attribute. A normalization procedure is employed to reduce computational effort and standardize the data Y^y within the range of 0 to 1. A range of methodologies can be employed to normalize data. The proposed method employs an appropriate min-max normalization mechanism. This technique generates a quantitative score from the supplied dataset into Y_nor within a range of [0, 1] via equation (1).

$$Y_{nor} = \frac{Y^{y} - Y_{min}}{Y_{max} - Y_{min}} \times [new\_max - new\_min] + new\_min \quad (1)$$

Here, $new_{max} = 1$ and $new_{min} = 0$is used. By using this method, all of the qualities have values between 0 and 1, or within that range.

C. Cryptographic encryption and decryption

A cryptographic approach to security in communication systems can effectively ensure protected information and secure communication. The smart grid incorporates electronic components featuring low-cost hardware. They can employ public key cryptography to adhere to the cryptographic approach of encryption and decryption processes. To guarantee data integrity and privacy within the smart grid, it is essential to develop an encryption and decryption approach. In cryptography, the original message or data, referred to as plain text, is encrypted using a key value, termed cipher text, and transmitted across a channel. The inverse operation, termed decryption, involves decoding the encrypted text to disclose the plaintext. It generates the original plaintext utilizing a private key and ciphertext. The subsequent algorithm delineates the IA-TACITA encryption methodology for data transfer between two smart grid nodes.

- Stage 1: Initially, the file's contents are read in plain text format, after which the character locations are randomly rearranged utilizing the primary permutations method and a specified key value.
- Stage 2: Each character possesses a corresponding ASCII value. Determine the plaintext character within the text file and utilize its corresponding ASCII value.
- Stage 3: Execute an XOR operation utilizing a key value of n bits.
- Stage 4: The concept of implementing the IA-TACITA approach has been recognized.
- Stage 5: Following the conversion of the value to binary using IA-TACITA logic.
- Stage 6: Apply a bit-reversal technique to the freshly generated binary string.
- Stage 7: Ascertain the equivalent decimal value for each binary string.
- Stage 8: The resulting Uni-code character is the encrypted text expressed as a decimal number.
- Stage 9: Execute all cryptographic procedures from stages 1 to 7 for the subsequent characters in the text document until the "End of File (EoF)" is reached.
- The recipient is tasked with decrypting the information. Cipher text denotes the text that has been encrypted via the IA-TACITA method at the transmission source. The receiver can decode the ciphertext using the same key and the procedure outlined below.

D. Optimization Algorithm

The firefly optimization technique depends on variations in luminosity and the development of allure. Utilizing the light output as a surrogate for the objective function, we may assess the firefly's overall attractiveness. The firefly's luminosity is optimized at a specific w by choosing the value J(w) α e(w). Relative attractiveness, represented by b, is determined by the behavior of adjacent fireflies and varies with the distance q_ji between flies j and i. As light propagates away from its source, a greater proportion is absorbed by the ambient air, resulting in diminished total intensity. Moreover, equation (2) illustrates that the intensity of J(q) fluctuates in accordance with the inverse square law, contingent upon the level of absorption.

$$J(q) = \frac{J_T}{q^2} \quad (2)$$

Where J_T is the total intensity, q is the separation between the light source and the observer, and γ is the absorption coefficient. Light intensity J fluctuates with distances q using the light absorption coefficientJ_T, as given in equation (3).
J_T denotes the total intensity, q represents the distance between the light source and the observer, and γ signifies the absorption coefficient. The light intensity J varies with distance q according to the light absorption coefficient J_T, as specified in equation (3).

$$J = Ioe^{-\gamma q} \quad (3)$$

Where $f^{(-\gamma q)}$ is the aggregate intensity of the source and distance. Jp is the original intensity of light. The inverse square law and the Is $\frac{J_t}{q_2}$ are coupled to protect the singularities at $q = 0$ and can be analysed in Gaussian form in equation (4) together with the impact of absorption.

$$J = Ioe^{-\gamma q^2} \quad (4)$$

According to equation (5), the attraction of a firefly β is proportional to the brightness of its light as seen by other fireflies.

$$\beta = \beta oe^{-\gamma q^2} \quad (5)$$

Where β is the firefly, β_o is the attraction, and $e^{-\gamma q^2}$ is the sum of the source and distance intensities. It is simple to calculate $\frac{1}{(1+q^2)}$ whenq $= 0$. As opposed to the exponential functions, The rough approximation of equation (5) is provided in equation (6).

$$\beta = \frac{\beta o}{1+\gamma q^2} \quad (6)$$

Where β is a firefly, β_o is the attractiveness of a firefly, γ is light absorption co-efficient, and q is the distance between source and light. Equations 5 and 6 explain the characteristics of distance $\frac{1}{\gamma}$ over the attractiveness by changing the βo significantly to $\beta oe^{(-1)}$. The attractive function will decrease as explained in equation (7) and the fixed characteristics of the length are explained in equation (8).

$$\beta(q) = \beta of^n (n \geq 1) \quad (7)$$

$$\tau = \gamma^{-\frac{1}{n}} \to 1, n \to \infty \quad (8)$$

In the optimization problem, the initial value γ for the target length isτ, where = $\gamma = \frac{1}{q^n}$. Cartesian distance, as demonstrated by equation 9, can be used to find the separation between the two fireflies.

$$q_{ji} = |W_j - W_i| \sqrt{\sum_{l=1}^{c} (w_{jl} - w_{i,l})^2} \quad (9)$$

Where $w_{i,}l$ is the l^{th} component of the spatial coordinate, W_j is the j^{th} firefly.
In this case, $w_{i,}l$ represents the l^{th} component of the spatial coordinate, whileW_j is the j^{th}firefly.

3. Result

This section assesses the efficacy of the existing and proposed methodologies. The parameters are encryption duration (ms), decryption duration (ms), security level (%), and throughput (Mbps). The current methodologies include LWQE [13], PPOA [14], and ARSA [15]. Security level denotes the evaluation of the likelihood that a security assessment will be conducted or has transpired. Figure 2 and Table 1 illustrate a comparative comparison of security levels in proposed and conventional methods. The proposed IA-TACITA exhibits a security level of 95%, surpassing the existing methods LWQE (93%), PPOA (93%), and ARSA (85%). The findings indicate that the proposed methodology IA-TACITA offers superior security compared to the previously employed methods LWQE, PPOA, and ARSA.

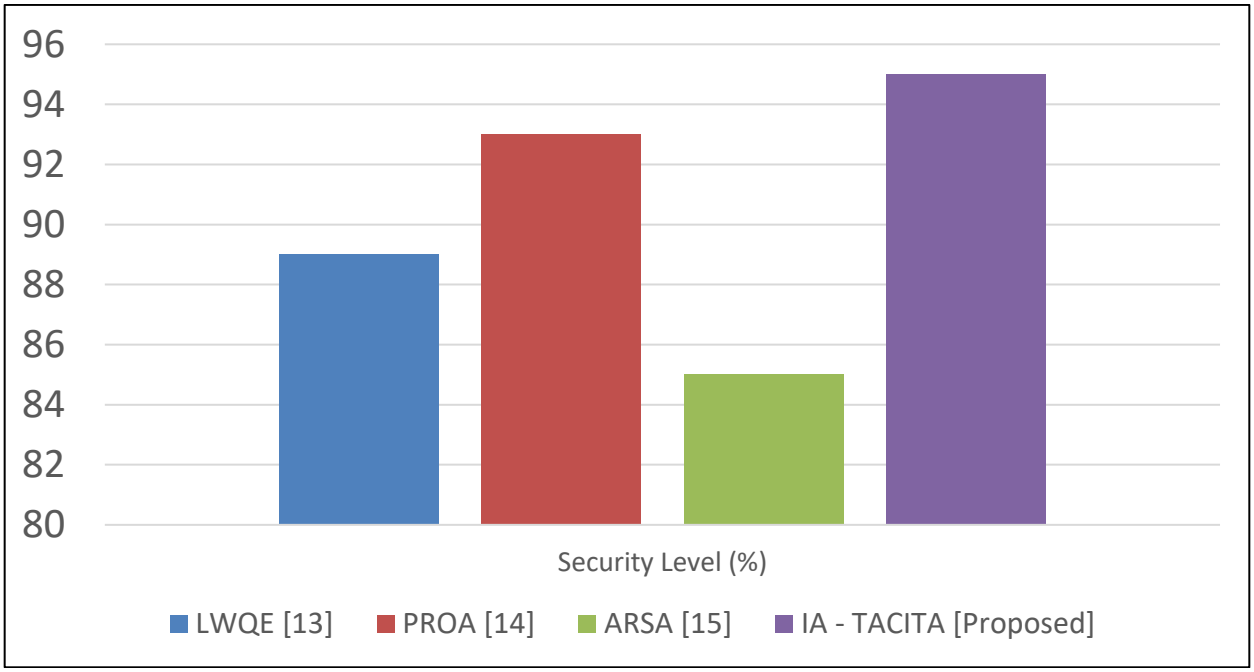

Figure 2: Comparison of Security level in the traditional and suggested method

Table 1: Comparison of security level

Methods	Security Level (%)
LWQE [13]	89
PROA [14]	93
ARSA [15]	85
IA - TACITA [Proposed]	95

The mean duration for data encryption is examined and presented in Encryption Time. The duration is expressed in milliseconds (ms). Figure 3 and Table 2 illustrate a comparative examination of encryption duration in proposed and conventional methods. The proposed IA-TACITA necessitates only 150 ms, whereas the current approaches LWQE, PPOA, and ARSA require 175 ms, 180 ms, and 160 ms, respectively. The IA-TACITA enhances security relative to existing approaches such as LWQE, PPOA, and ARSA.

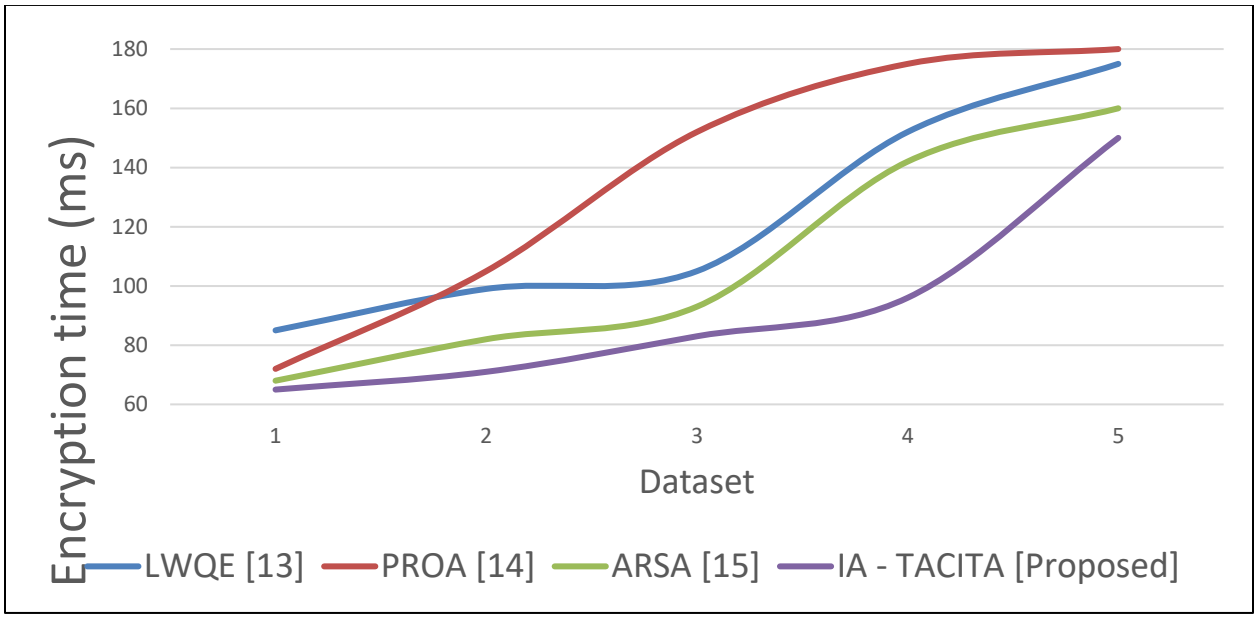

Figure 3: Comparison of encryption time in the traditional and suggested method

Table 2: Comparison of encryption time

Dataset	Encryption time (ms)			
	LWQE [13]	PROA [14]	ARSA [15]	IA - TACITA [Proposed]
1	85	72	68	65
2	99	105	82	71
3	105	152	93	83
4	152	175	142	96
5	175	180	160	150

The procedure of reverting encrypted material to its original form is referred to as decryption. A prevalent technique is reverse encryption. Encrypted data is accessible just to authorized individuals, as decryption necessitates a secret key or password. It is quantified in milliseconds (ms). Figure 4 illustrates a comparative examination of decryption times between the proposed and traditional methods. In contrast to the existing methods LWQE, PPOA, and ARSA, which have decryption times of 220 ms, 215 ms, and 225 ms, respectively, the proposed IA-TACITA requires just 190 ms. Consequently, the IA-TACITA demonstrates superior efficiency compared to existing methodologies such as LWQE, PPOA, and ARSA.

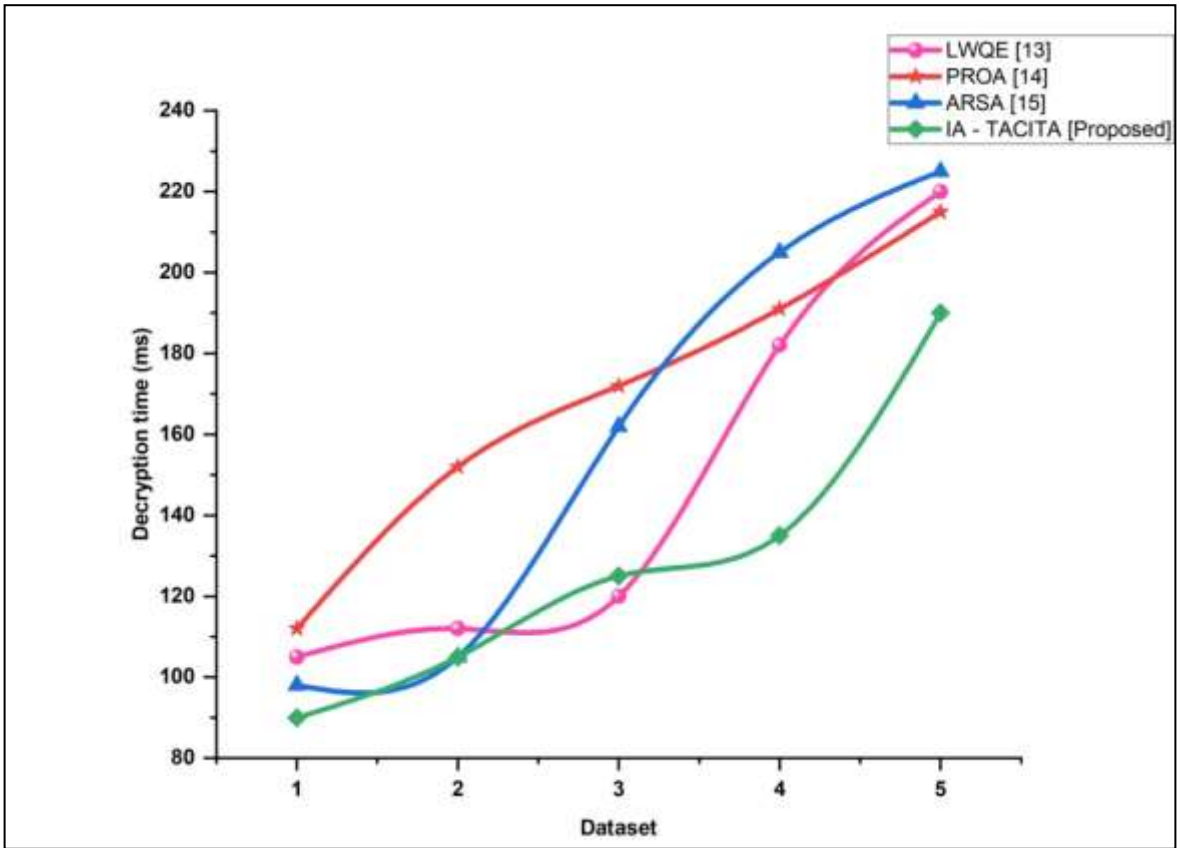

Figure 4: Comparison of decryption time in the traditional and suggested method

Table 3: Comparison of decryption time

Dataset	Decryption time (ms)			
	LWQE [13]	PROA [14]	ARSA [15]	IA - TACITA [Proposed]
1	105	112	98	90
2	112	152	105	105
3	120	172	162	125
4	182	191	205	135
5	220	215	225	190

Throughput refers to the rate at which a system processes or transmits data within a designated timeframe. Megabytes per second (Mbps) is the unit of measurement for the data transfer rate from the server to users. Figure 5 illustrates a comparative examination of throughput between the suggested and traditional methods. The proposed IA-TACITA achieves a throughput of 6.5 Mbps, which markedly exceeds the present approaches LWQE (4.2 Mbps), PPOA (3.5 Mbps), and ARSA (5.8 Mbps). The efficacy of the proposed methodology IA-TACITA for information transmission or processing significantly surpasses that of the current methods LWQE, PPOA, and ARSA.

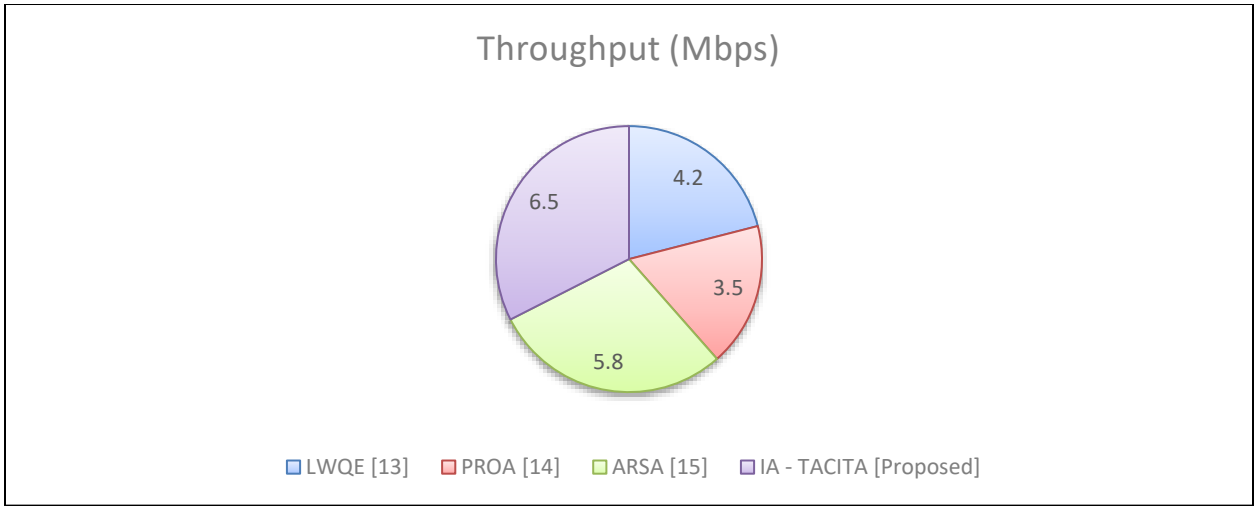

Figure 5: Comparison of throughput in the traditional and suggested method

Table 4: Comparison of throughput

Methods	Throughput (Mbps)
LWQE [13]	4.2
PROA [14]	3.5
ARSA [15]	5.8
IA - TACITA [Proposed]	6.5

4. Conclusion

Smart grids are digitally-enabled modern technologies that can enhance electricity generation while reducing power interruptions. The incorporation of information and contemporary communication technologies into the electrical grid has been identified as the optimal approach for enhancing the grid's architecture in IoT. Diverse energy production systems communicate, facilitating consensus and enabling informed, deliberative decision-making. The key focus is on the distribution endpoint of the grid's security in IoT. The study primarily focused on security risks related to an Internet of Things-based smart grid. Integrating a gadget proficient in cryptography encryption and decryption will resolve the issues. Algorithms such as AES, DES, XMODES, and RC5 impose specific limitations on key size and block size. In comparison to other encryption and decryption approaches, the integration of IA-TACITA has demonstrated superior outcomes. Regrettably, a sufficiently extensive dataset to analyze the cryptographic algorithms employed in IoT-based smart grids is not currently available. Extensive datasets will be necessary for the processing of cryptographic algorithms in the future.

Reference

1. Ghiasi, M., Wang, Z., Mehrandezh, M., Jalilian, S. and Ghadimi, N., 2022. Evolution of smart grids towards the Internet of energy: Concept and essential components for deep decarbonisation. IET Smart Grid.
2. Albesher, A.A., 2019. Iot in health-care: Recent advances in the development of smart cyber-physical ubiquitous environments. IJCSNS, 19(2), p.181.
3. Ang, L.M., Seng, K.P. and Wachowicz, M., 2022. Embedded intelligence and the data-driven future of application-specific Internet of Things for smart environments. International Journal of Distributed Sensor Networks, 18(6), p.15501329221102371.
4. Diwan, S.A., 2022. Dynamic Lightweight Mechanism for Security and Performance in Internet of Things. International Journal of Interactive Mobile Technologies, 16(10).

5. Lee, S. ., Kim, J. and Shon, T (2016) User privacyenhanced security architecture for home area network of Smart grid. Multimedia Tools and Applications, Springer Vol. 75(20), pp (12749-12764).
6. Priya, S.S. Karthigaikumar, P., Mangai, N.S. and Das, P.K.G. (2017) An efficient hardware architecture for high throughput AES encryptor using MUX based sub pipelined S-box. Wireless Personal Communications, Springer Vol. 94(4), pp (2259-2273).
7. Zodpe, H. and Sapkal, A (2018). An efficient AES implementation using FPGA with enhanced security features. Journal of King Saud University-Engineering Sciences, Elsevier pp (1-8).
8. P. Gope and B. Sikdar, "Lightweight and Privacy-Friendly Spatial Data Aggregation for Secure Power Supply and Demand Management in Smart Grids," IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1554–1566, 2019.
9. V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1900–1910, 2018.
10. A. Abdallah and X. S. Shen, "A Lightweight Lattice-Based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid," IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 396–405, 2018
11. P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks," IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 4349–4359, 2019.
12. Al-Hawawreh, M., Moustafa, N., Garg, S. and Hossain, M.S., 2020. Deep learning-enabled threat intelligence scheme in the internet of things networks. IEEE Transactions on Network Science and Engineering, 8(4), pp.2968-2981.
13. Li, Y., Zhang, P. and Huang, R., 2019. Lightweight quantum encryption for secure transmission of power data in smart grid. IEEE Access, 7, pp.36285-36293.
14. Zhai, F., Yang, T., Zhao, B. and Chen, H., 2022. Privacy-Preserving Outsourcing Algorithms for Multidimensional Data Encryption in Smart Grids. Sensors, 22(12), p.4365.
15. Wang, F., Wang, Z. and Zhu, Y., 2019, August. Adaptive RSA encryption algorithm for smart grid. In Journal of Physics: Conference Series (Vol. 1302, No. 2, p. 022097). IOP Publishing.