International Journal for Modern Trends in Science and Technology
Volume 10, Issue 04, pages 410-414.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue04.html
DOI: https://doi.org/10.46501/IJMTST1004064

# Enhanced Security and Routing for IoT-Based Smart Grids: 32-Bit Key Management and Fuzzy Techniques

**R. R. Ramya[1], Banumathi J[2]**

[1]Research Scholar, Department of Information Technology, University College of Engineering, Nagercoil, Tamilnadu, India.
[2]Assistant Professor, Department of Information Technology, University College of Engineering, Nagercoil, Tamilnadu, India.

**To Cite this Article**
R. R. Ramya and Banumathi J, Enhanced Security and Routing for IoT-Based Smart Grids: 32-Bit Key Management and Fuzzy Techniques, International Journal for Modern Trends in Science and Technology, 2024, 10(04), pages. 410-414. https://doi.org/10.46501/IJMTST1004064

**Article Info**
Received: 11 April 2024; Accepted: 27 April 2024; Published: 30 April 2024.



## ABSTRACT

***The Smart Grid represents a cutting-edge solution that harnesses digital progress and advanced communication networks to observe and adjust to changes in electricity consumption. Its primary objective is to revolutionize the methods through which electricity is distributed, transmitted and produced. In the process of transmitting and distributing parameters, there is a risk of data loss or interception. For addressing this issue, an improved security and routing system has been implemented for IoT-based smart grids. This system utilizes 32-bit key management and a fuzzy technique to enhance protection against potential threats. By utilizing this method, the parameters are effortlessly transmitted and the efficiency of the intelligent grid system is evaluated using MATLAB software. The results show a significant improvement in throughput compared to artificial neural networks (ANN) and genetic algorithms (GA), with a packet delivery ratio increased to 96% when compared to alternative techniques.***

***Keywords: Smart grid, Routing, Fuzzy, Artificial Neural Network, Genetic algorithm, Matlab, Efficiency.***

## 1. INTRODUCTION

Today's electrical networks consist of a multitude of power generation nodes, including coal-fired plants, gas-fired plants, hydroelectric plants and more. It is important to mention that most of the equipment and wiring in the conventional power grid has been in operation for an extended period [1]. An electric grid, also known as a power grid which is a complex network of interconnected systems that facilitate the distribution of electricity from power producers to consumers. The conventional electrical grid system has been in place for over a century without any notable enhancements to its basic infrastructure. Despite the significant increase in electricity demand in recent decades, there has been a lack of progress in managing and controlling electricity consumption and production on a larger scale [2]. Estimating the state of the system is crucial for the efficient operation of the Energy Management System (EMS) within the Internet of Things (IoT) enabled smart grid. The energy management system is utilized for various functions including control, scheduling and decision-making processes such as automatic generation control, optimal power flow and economic dispatch [3]. The IoT is a rapidly evolving technology sector that are

divided into three main categories,

1) Utilizing Internet technologies to connect smart devices and objects.

2) The integration of various technologies to enhance internet services includes Radio Frequency Identification (RFID), Machine-to-Machine (M2M) communication, as well as sensors and actuators.

3) Combining various applications with services has the potential to create fresh opportunities in both the business and market sectors.

An imbalance in the network leads to a rise in the neutral current flow, resulting in an increase in the expenses associated with the neutral conductor [4]. The increasing attack surfaces in IoT have brought about a multitude of cyber-security challenges. These challenges stem from the inherent vulnerabilities within the system, leaving it susceptible to various attacks [5]. The term key management encompasses the administration of cryptographic keys within a cryptographic system. It involves the design of cryptographic protocols, key servers, user guidelines and other pertinent protocols. Fuzzy logic is a method of reasoning that allows for multiple values based on the degree of truth, rather than the binary true or false approach of Boolean logic. Unlike traditional approaches, the fuzzy integral is capable of integrating multiple fuzzy sets into a comprehensive fuzzy measure space. This unique feature allows for the integration of fuzzy sets without the requirement of a common approximation [6-8]. The advancement in secure encryption techniques with energy optimization using a random permutation pseudo algorithm based on the Internet of Things in wireless sensor networks has shown superior performance compared to traditional algorithms like GKA and MPKE. Not only in performance, has it enhanced the data traffic and throughput rate through stable routing. However, Wireless Sensor Networks (WSN) with limited resources are not efficient and consume a lot of energy [9]. The grid-based routing model proposed earlier aims to enhance the energy efficiency and security of data transmission in WSNs used in smart building applications. This method offers a reliable and secure routing protocol specifically designed for WSNs in smart buildings. But still, the mean remaining energy in the new system reached 96%, with potential for even higher levels in future enhancements [10]. In accordance with the previously mentioned method, the subsequent approach suggests a hierarchical strategy for handling keys to safeguard various WSNs through the use of Hybrid Energy-Efficient Distributed (HEED) routing. The key management system makes use of the Bloom scheme and a pseudo-random number generator (PRNG) to effectively create keys while preserving sensor resources. The suggested approach offers enhanced security, adaptability, scalability and energy efficiency and additionally, the goal is to expand the utilization of WSN in IoT applications. However, this will necessitate further testing for vulnerabilities and evaluating performance using contemporary methodologies [11-12]. A highly effective authentication protocol has been developed for smart grid communication, utilizing on-chip-error-correcting physical unclonable function technology. This protocol offers significant benefits such as enhancing the overall performance of the power grid, efficiency and reliability, while also strengthening security measures to protect against potential cyber-attacks. Regulatory compliance remains a key challenge in implementing this advanced protocol [13-14]. The protocol introduces a secure method for smart meters to authenticate with the USP while minimizing communication and computation overhead. Further research is needed to formally verify the security aspects of the protocol and assess its performance using additional metrics not covered in this existing system [15].

The limitations of the systems mentioned above include decreased performance, energy efficiency and regulatory compliance. In order to address these issues, a new technique called Enhanced Security and Routing for IoT-Based Smart Grids: 32-Bit Key Management and Fuzzy Techniques has been introduced. This innovative approach utilizes both key management and fuzzy techniques to determine the shortest and most secure path for data transmission.

## 2. PROPOSED SYSTEM

Smart grids are developed with the intention of reducing overall expenses by utilizing smart energy IoT monitoring and redirecting energy sources to quickly restore power in the event of a blackout. To improve the stability of the grid, promoting optimal energy consumption and incorporating sustainable energy sources, the technique moves0 to the system of 32-bit key management and fuzzy technique for enhancing and

securing IoT-Based smart grids.

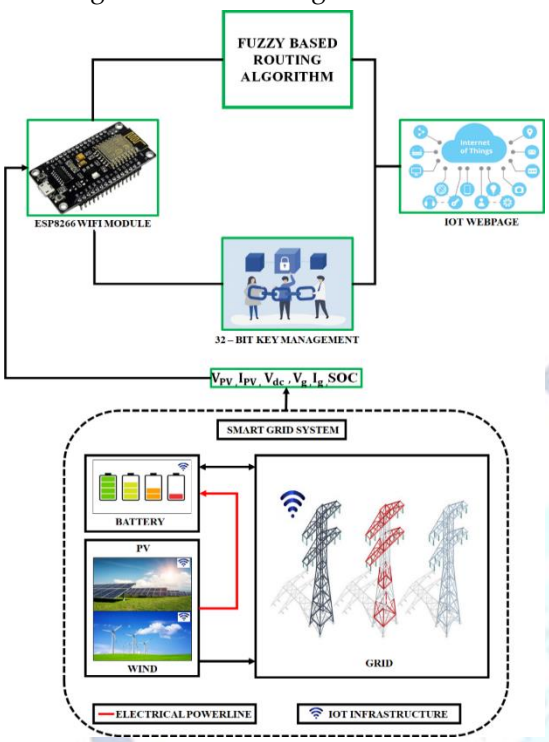



Figure 1: Block Diagram of the proposed system

The advanced grid system is made up of three key components including batteries, solar panels and wind turbines. The data produced by these components is measured in terms of Vpv, Ipv, Vdc and SOC. This data is collected and analyzed by a device known as the ESP8266 WiFi module. The module shows the voltage and current readings, which are then transmitted to the IoT web page. Prior to sending the data to the smart grid, the module collects and displays the information on an IoT web page. As the data passes from the module to the web page, two processes are initiated. The first process involves fuzzy-based routing to determine the most efficient path, while the second process focuses on securing the data using a 32-bit key management system.

## 3. PROPOSED SYSTEM MODELING

### SMART GRID SYSTEM:

The Smart Grid is an innovative technology that utilizes digital advancements and sophisticated communication systems to monitor and adapt to fluctuations in electricity usage. Its main goal is to transform the way power is distributed, transmitted and generated. It works to bring together the requirements and abilities of various generators, grid operators, consumers and electricity market participants in order to run the entire system in the most efficient manner possible. This is done in order to reduce costs and minimize environmental impacts, while at the same time maximizing the reliability, resilience, flexibility and stability of the system.

### ESP8266 WiFi Module:

The ESP8266 WiFi Module is a powerful System-On-a-Chip (SOC) with a built-in TCP/IP protocol stack, enabling seamless connectivity to the WiFi network for any microcontroller. This versatile module that serves as a standalone application host or handle all WiFi networking tasks for another processor. The ESP8266 module is known for its affordability and is favoured by a large and continuously expanding group of users.

### FUZZY BASED ROUTING:

Utilizing fuzzy logic in routing protocols, specifically within ad-hoc wireless networks and networks that cater to different quality of service levels, is known as fuzzy routing. The fuzzy technique is employed to determine the optimal and most efficient route to minimize both time spent and energy consumed during travel. Figure 2, shows the architecture of fuzzy based routing.

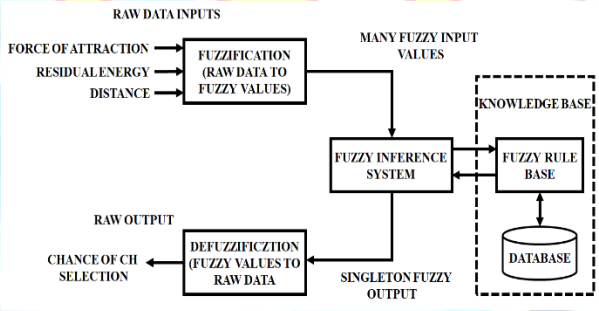



Figure 2: Architecture of Fuzzy Based Routing

### 32-Bit Key Management:

The process of key management helps to ensure confidentiality and protection by overseeing how keys are distributed and taking prompt action if an encrypted radio device is misplaced or stolen. If an unauthorized individual gains possession of a lost or stolen radio, it could potentially jeopardize the security of the entire Land Mobile Radio (LMR) system. The most secure way to handle cryptographic keys is by utilizing a Hardware Security Module (HSM) or CloudHSM. In cases where an HSM is not being utilized, the keys that are securely stored on the client's premises or if being used on the Cloud, the Cloud Service Provider's Key Management Service is employed. Figure 3 illustrates the block diagram of cryptographic key management system.

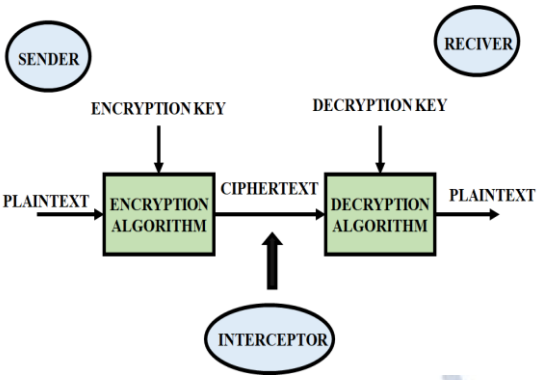



Figure 3: Block Diagram of Cryptographic Key Management

**IoT Webpage:**

The term IoT, short for Internet of Things, encompasses a network of interconnected devices and the technology that enables communication between these devices and the cloud, as well as among the devices themselves. An average IoT system operates by continuously gathering and sharing data in real-time. IoT system has three components:

1. Smart devices
2. Iot applications
3. Graphical user interface

## 4. RESULTS AND DISCUSSION

In this paper, the enhancement of security and routing for Iot based smart grid system using 32-bit key management system and fuzzy technique has been introduced. The effectiveness of the proposed smart grid system is assessed with MATLAB, while the data from sensors is showcased through the Adafruit web app.

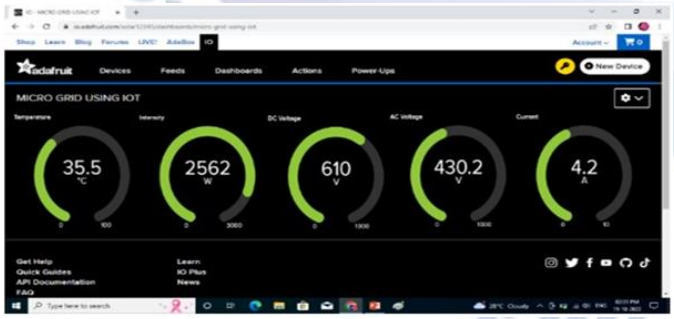
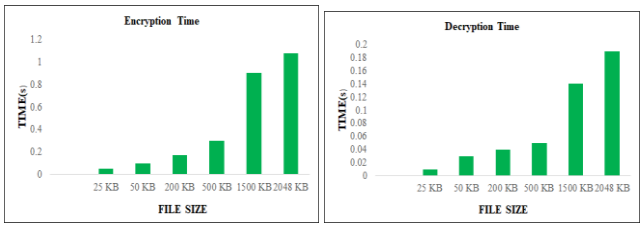



Figure 4: Output obtained using Matlab

The findings depicted in Figure 4 show the outcomes achieved through the utilization of Matlab in improving routing and security measures for the IoT smart grid. This was accomplished by implementing a 32-bit key management system in combination with a fuzzy technique.




(a) (b)

Figure 5: (a) Encryption Time & (b) Decryption Time

The chart in Figure 5(a) displays the amount of time it takes to encrypt each file size. Among the different file sizes, it is evident that encrypting a 2048 KB file takes significantly longer compared to others. On the other hand, encrypting a 25 KB file requires much less time for the same encryption process and Figure 5(b) displays the amount of time it takes to decrypt each file size. Among the different file sizes, it results that decrypting a 2048 KB file takes significantly longer compared to others. On the other hand, decrypting a 25 KB file requires much less time for the same decryption process.

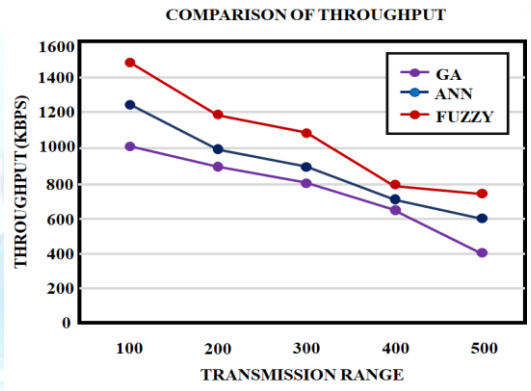



Figure 6: Comparison of Throughput performance

The graph in Figure 6 illustrates the differences in throughput performance among three distinct techniques: fuzzy logic, Artificial Neural Networks (ANN) and Genetic Algorithms (GA). The results clearly indicate that the proposed system, Fuzzy has significantly enhanced throughput across all transmission ranges when compared to both GA and ANN.

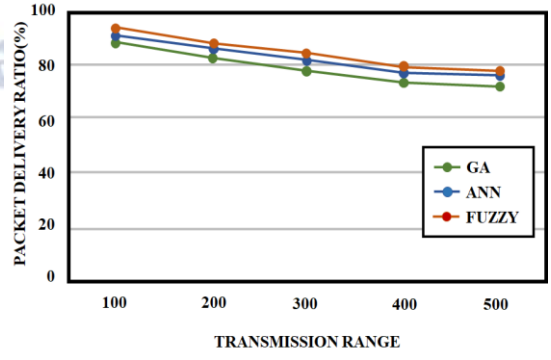



Figure 7: Comparison of Packet delivery ratio

Figure 7 shows a comparison of packet delivery ratios among Fuzzy, ANN and GA. At a transmission range of 100, the packet delivery ratios are 87% for GA, 90% for ANN and 96% for fuzzy. This comparison reveals that the fuzzy technique in the proposed system performs better for each transmission range.

## 5. CONCLUSION

In this paper, a novel approach utilizing fuzzy technique and 32-bit key management is proposed to enhance the security and routing system. The main goal is to improve the throughput and data delivery ratio by identifying various types of network algorithms. The smart grid system incorporates information from both PV and Wind energy datasets, with parameters being showcased in a Wi-Fi module. Prior to transferring the IoT webpage, two processes are involved: a fuzzy-based algorithm and a 32-bit key management system. The time required for both encryption and decryption processes increases with larger file sizes. When compared to ANN and GA, fuzzy technique shows better performance in terms of throughput. Moreover, in regards to packet delivery ratio, fuzzy technique achieves an impressive 96% ratio with corresponding transmission ranges. The effectiveness of the suggested smart grid system is assessed using MATLAB, while the sensors track various parameters that are then visualized through the Adafruit web application.

## Conflict of interest statement

Authors declare that they do not have any conflict of interest.

## REFERENCES


[1] Alomar, Madani Abdu. "An IOT based smart grid system for advanced cooperative transmission and communication." Physical Communication 58 (2023): 102069.

[2] M. U. Saleem, M. R. Usman, M. A. Usman and C. Politis, "Design, Deployment and Performance Evaluation of an IoT Based Smart Energy Management System for Demand Side Management in Smart Grid," in IEEE Access, Vol. 10, pp. 15261-15278, 2022.

[3] Z. Zhang, R. Deng, D. K. Y. Yau and P. Chen, "Zero-Parameter-Information Data Integrity Attacks and Countermeasures in IoT-Based Smart Grid," in IEEE Internet of Things Journal, Vol. 8, no. 8, pp. 6608-6623, 15 April15, 2021.

[4] M. R. Islam, H. Lu, M. R. Islam, M. J. Hossain and L. Li, "An IoT-Based Decision Support Tool for Improving the Performance of Smart Grids Connected With Distributed Energy Sources and Electric Vehicles," in IEEE Transactions on Industry Applications, Vol. 56, no. 4, pp. 4552-4562, July-Aug. 2020.

[5] Anand, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Felseghi, R.A.; Raboaca, M.S. IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. Energies 2020, 13, 4813.

[6] El-Khamy, Said E., Noha O. Korany, and Amira G. Mohamed. "A new fuzzy-DNA image encryption and steganography technique." IEEE Access 8 (2020): 148935-148951.

[7] Arumugam, Maharajan, and Kumar Parasuraman. "Whale optimized routing path selection and 128 bit secured key management for maritime safety." International Journal of Naval Architecture and Ocean Engineering (2024): 100584.

[8] M. F. Moghadam, M. Nikooghadam, M. A. B. A. Jabban, M. Alishahi, L. Mortazavi and A. Mohajerzadeh, "An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network," in IEEE Access, Vol. 8, pp. 73182-73192, 2020.

[9] Nagaraj, S.; Kathole, A.B.; Arya, L.; Tyagi, N.; Goyal, S.B.; Rajawat, A.S.; Raboaca, M.S.; Mihaltan, T.C.; Verma, C.; Suciu, G. Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks. Energies 2023, 16, 8.

[10] Sivasankarareddy, V.; Sundari, G.; Rami Reddy, C.; Aymen, F.; Bortoni, E.C. Grid-Based Routing Model for Energy Efficient and Secure Data Transmission in WSN for Smart Building Applications. Appl. Sci. 2021, 11, 10517.

[11] Muhajjar, R.A.; Flayh, N.A.; Al-Zubaidie, M. A Perfect Security Key Management Method for Hierarchical Wireless Sensor Networks in Medical Environments. Electronics 2023, 12, 1011.

[12] Sujanthi, S., and S. Nithya Kalyani. "SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT." Wireless Personal Communications 114.3 (2020): 2135-2169.

[13] Kaveh, Masoud et al. "An efficient authentication protocol for smart grid communication based on on-chip-error-correcting physical unclonable function." Sustainable Energy, Grids and Networks 36 (2023): 101228.

[14] Appasani, Bhargav, et al. "Blockchain-enabled smart grid applications: Architecture, challenges, and solutions." Sustainability 14.14 (2022): 8801.

[15] Amanlou, Sanaz, Mohammad Kamrul Hasan and Khairul Azmi Abu Bakar. "Lightweight and secure authentication scheme for IoT network based on publish–subscribe fog computing model." Computer Networks 199 (2021): 108465.