ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

INNOVATIVE ENERGY-EFFICIENT PROXY REENCRYPTION FOR SECURE DATA EXCHANGE IN WIRELESS SENSOR NETWORKS

ROJARAMANI ADAPA[1], BADDAM DIMPUL REDDY[2], GANGONI SAI PAVAN[3], B V THARUN TEJA REDDY[4], BACHU BHANU PRASAD[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In the realm of wireless sensor networks (WSNs), preserving data integrity, privacy, and security against cyberthreats is paramount. Proxy re-encryption (PRE) plays a pivotal role in ensuring secure intra-network communication. However, existing PRE solutions encounter persistent challenges, including processing delays due to the transfer of substantial data to the proxy for re-encryption and the computational intensity of asymmetric cryptography. This study introduces an innovative PRE scheme that is meticulously customized for WSNs to enhance the secure communication between nodes within the network and external data server. The proposed PRE scheme optimizes efficiency by integrating lightweight symmetric and asymmetric cryptographic techniques, thereby minimizing computational costs during PRE operations and conserving energy for resource-constrained nodes. In addition, the scheme incorporates sophisticated key management and digital certificates to ensure secure key generation and distribution, which in turn, facilitates seamless authentication and scalable data sharing among the entities in WSN. This scheme maintains sensor-node data encryption and delegates secure re-encryption tasks exclusively to cluster heads, thereby reinforcing data privacy and integrity. Comprehensive evaluations of

security, performance, and energy consumption validated the robustness of the scheme. The results confirm that the proposed PRE scheme significantly enhances the security, efficiency, and overall network lifetime of WSNs.

Index Terms – Proxy Re-Encryption, Wireless Sensor Networks, Energy Efficiency, Secure Data Exchange, Cryptography, Key Management, IoT Security, Secure Communication, Access Control, Cybersecurity.

I. INTRODUCTION

Wireless sensor networks (WSNs) represent a pivotal technological advancement in an increasingly interconnected world. These networks comprise a multitude of resource-constrained small sensor devices that collaborate to collect and exchange data from their immediate surroundings. This collaborative capability enables WSNs to find applications in diverse fields ranging from environmental monitoring and surveillance to industrial automation and healthcare systems. However, sensor nodes (SNs) inherently face limitations, such as constraints in computational power, energy resources, memory, and bandwidth. These limitations give rise to multifaceted challenges in the intricate task of sharing information within a network, amplifying the significance of ensuring data security and confidentiality. In addition, SNs are vulnerable to various types of attacks, including physical tampering, data interception, node compromise, and denial-of-service (DoS) attacks. These SNs which are deployed remotely and left unmonitored, are particularly susceptible to these threats. Attackers may tamper with SNs to compromise their functionality, steal valuable data, or disable them, to disrupt network operations. Data interception attacks can lead to breaches of data confidentiality, exposing sensitive information to unauthorized entities. Node-compromise attacks can compromise data integrity, and DoS attacks can disrupt network communication and availability. Information privacy and integrity are paramount concerns during communication and sharing among SNs, cluster heads (CHs) and base stations (BSs). Traditional security mechanisms deployed in WSNs often rely on intricate cryptographic calculations. Unfortunately, these mechanisms impose a considerable energy burden on the SNs, severely hindering communication efficiency. Given the intrinsic energy limitations of SNs, this excessive energy consumption has the

potential to cause nodes to deplete their power, potentially leading to premature failure, thus curtailing the network's operational lifetime. In particular, real-time applications are highly sensitive to these energy inefficiencies because they require low latency for rapid decision making. Proxy re-encryption (PRE) technology enables secure data communication and sharing within a network, whereby a semi-trusted proxy is employed to convert encrypted data from one device to another without exposing the actual content or any private keys. This seamless transformation is achieved using a re-encryption key provided by a trusted third party that ensures that the data remain confidential and secure throughout the entire transfer process. However, PRE is most effective when large resource-rich devices are employed. and significantly less efficient when deployed on resource-constrained devices, such as SNs. The primary reason for this reduced efficiency stems from the substantial computational costs associated with the complex cryptographic calculations required by the PRE process. These resource-intensive computations render PRE less suitable for devices with limited computational capabilities and energy resources. Additionally, as data-sharing volumes increase and involve a larger number of devices, the computational workload of the proxy escalates, potentially leading to delays in the re-encryption process, which could affect the overall network efficiency and real-time data transmission.

II. RELATED WORK

A. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks

In wireless sensor networks (WSNs), security, efficiency, and energy consumption are still major challenges due to its open, large-scale, and resource-constrained nature. The 6LoWPAN protocol and many other lightweight cryptographic methods have been developed to improve the security and efficiency of WSNs with a reasonable amount of energy and resource utilization. However, they still suffer from limitations in terms of flexibility, key management, authentication, and the power resource management processes. This paper addresses these issues by designing FlexCrypt, an automated lightweight cryptographic scheme for WSNs. In the FlexCrypt scheme, a new dynamic clustering technique that supports mobility among the sensor nodes is developed. Moreover, the proposed scheme

introduces a flexible lightweight cryptographic method to control the complexity of the encryption by automating the selection of encryption parameters based on the presently available resources of each sensor node to encrypt the data. In addition, a new lightweight key management and authentication method is designed to establish secure communication and the exchange of data and keys among the various WSN nodes. The proposed FlexCrypt scheme was evaluated using the Cooja simulator with Contiki OS. The results prove that the proposed scheme provides a significant improvement in terms of delay and encryption time in addition to power consumption and network lifetime compared to other ciphers that use fixed encryption parameters. It can effectively extend the network lifetime by 86%, 94% and 90% compared to the FlexenTech, AES and TEA ciphers, respectively. The security analysis demonstrates that the FlexCrypt scheme can resist various attacks such as brute-force, eavesdropping, man-in-the-middle and replay attacks.

B. Blockchain-based decentralized authentication model for IoT-based E-learning and educational environments

In recent times, technology has advanced significantly and is currently being integrated into educational environments to facilitate distance learning and interaction between learners. Integrating the Internet of Things (IoT) into education can facilitate the teaching and learning process and expand the context in which students learn. Nevertheless, learning data is very sensitive and must be protected when transmitted over the network or stored in data centers. Moreover, the identity and the authenticity of interacting students, instructors, and staff need to be verified to mitigate the impact of attacks. However, most of the current security and authentication schemes are centralized, relying on trusted third-party cloud servers, to facilitate continuous secure communication. In addition, most of these schemes are resource-intensive; thus, security and efficiency issues arise when heterogeneous and resource-limited IoT devices are being used. In this paper, we propose a blockchain-based architecture that accurately identifies and authenticates learners and their IoT devices in a decentralized manner and prevents the unauthorized modification of stored learning records in a distributed university network. It allows students and instructors to easily migrate to and join multiple universities within the network using their identity without the need for user re-authentication.

The proposed architecture was tested using a simulation tool, and measured to evaluate its performance. The simulation results demonstrate the ability of the proposed architecture to significantly increase the throughput of learning transactions (40%), reduce the communication overhead and response time (26%), improve authentication efficiency (27%), and reduce the IoT power consumption (35%) compared to the centralized authentication mechanisms. In addition, the security analysis proves the effectiveness of the proposed architecture in resisting various attacks and ensuring the security requirements of learning data in the university network.

C. The determinants of reliable smart grid from experts' perspective

A smart grid integrates communication networks with the conventional electrical grid. Due to their potential, smart grids are anticipated to achieve widespread deployment. A key component of the success and adoption of smart grids is reliability. Without knowing users' impressions of the reliability of the smart grid, users will not easily accept and participate in it or its services. However, very few studies address smart grid reliability from the perspective of users. Thus, there is a urgent need to identify key factors that affect smart grid reliability from the user's viewpoint. The goal of this paper is to examine user perceptions of smart grid reliability and assess their success factors in an effort to close the gap in the literature. This paper propose a model to investigate and determine the most crucial factors that affect the smart grid's reliability based on the Multiple-criteria decision-making (MCDM) method. Firstly, a comprehensive literature analysis was conducted to determine the criteria and sub-criteria used to construct the model; then, the model is constructed using fifteen sub-criteria covering big data, network systems, and grid efficiency criteria; finally, the Fuzzy Analytic Hierarchy Approach (FAHP) and fuzzy triangular numbers are used to evaluate and prioritize the criteria. Twenty smart grid experts were consulted to collect data. The results indicate the significance of the 'Big Data' criterion, closely followed by 'Grid Efficiency' criterion. Additionally, it is discovered that the sub-criteria of 'Privacy' and 'Interoperability' had a significant impact on the reliability of the smart grid. The sensitivity analysis shows the variation of factors ranking and the stability and robustness of the model and the results. The research presented in this study has practical applications for academics, engineers, decision-makers, and stakeholders.

III. PROPOSED METHODOLOGY

The proposed PRE scheme optimizes efficiency by integrating lightweight symmetric and asymmetric cryptographic techniques, thereby minimizing computational costs during PRE operations and conserving energy for resource-constrained nodes. In addition, the scheme incorporates sophisticated key management and digital certificates to ensure secure key generation and distribution, which in turn, facilitates seamless authentication and scalable data sharing among the entities in WSN. This scheme maintains sensor-node data encryption and delegates secure re-encryption tasks exclusively to cluster heads, thereby reinforcing data privacy and integrity. Comprehensive evaluations of security, performance, and energy consumption validated the robustness of the scheme.

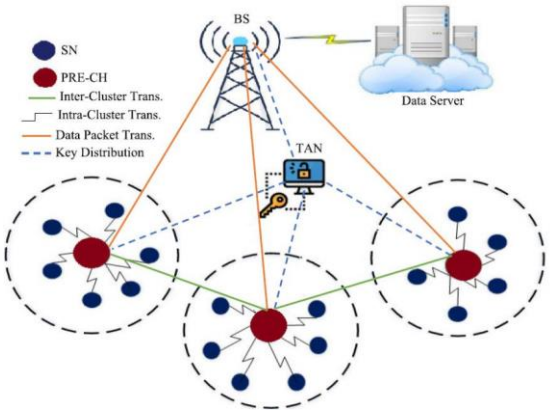


Fig. 1: System Overview

1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else, user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

2. Sensor Nodes (SNs)

However, sensor nodes (SNs) inherently face limitations, such as constraints in computational power, energy resources, memory, and bandwidth. These limitations give rise to multifaceted challenges in the intricate task of sharing information within a network, amplifying the significance of ensuring data security and confidentiality. In particular, real-time applications are highly sensitive to these energy inefficiencies because they require low latency for rapid decision making.

3. Cluster Heads (CHs) and Base Stations (BSs)

Information privacy and integrity are paramount concerns during communication and sharing among SNs, cluster heads (CHs)

and base stations (BSs). Traditional security mechanisms deployed in WSNs often rely on intricate cryptographic calculations. Unfortunately, these mechanisms impose a considerable energy burden on the SNs, severely hindering communication efficiency.

4. Data Server

Data server responsible for receiving the data. The procedure also involves the creation of the re-encryption key (rk), which is used by a CH to re-encrypt a message between A and B. This flexibility in recipient types underscores the scalability and adaptability of the system, enabling secure data transmission and data sharing across a wide range of network entities. data servers, a secure connection is established through the associated CH.

5. Trusted Authority Node (TAN).

Given the resource-constrained nature of the CH, where resource-intensive tasks such as key generation, encryption, and re-encryption may deplete the power reserves, a specific fog/edge server with higher processing capabilities connected to all CHs, is designated as a fully trusted authority node (TAN). The TAN plays a pivotal role in overseeing the critical functions within the network. Its responsibilities include SN registration, generation of public system parameters, and the secure creation of cryptographic keys for each CH and its associated SNs. In addition, it is responsible for generating digital signatures to ensure the authentication of each node within the network. Notably, although TAN plays a central role in upholding network security, it remains entirely uninvolved in any aspect of PRE functionality.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the proxy re-encryption mechanism enabled secure data sharing between sensor nodes and authorized users without requiring repeated data encryption by the original sender. This significantly reduced computational workload and energy usage on resource-constrained sensor devices.

The analysis showed that the proposed approach achieved lower communication and processing overhead compared to traditional encryption-based data sharing methods while maintaining strong data confidentiality and access control. Furthermore, the energy optimization techniques extended network lifetime and improved scalability as the number of sensor nodes increased.

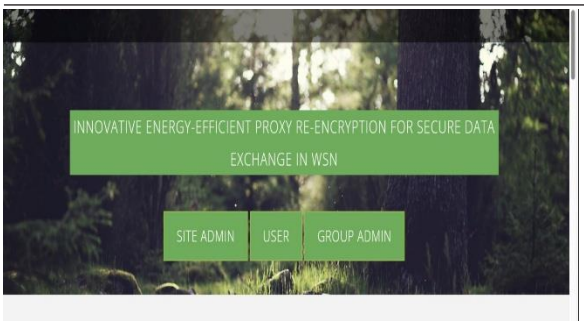


Fig. 2: Homepage



Fig. 3: Create New Group

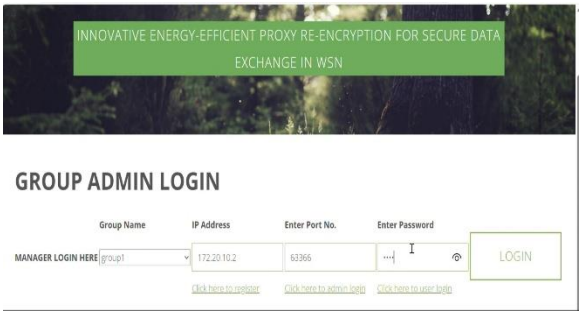


Fig. 4: Admin Login

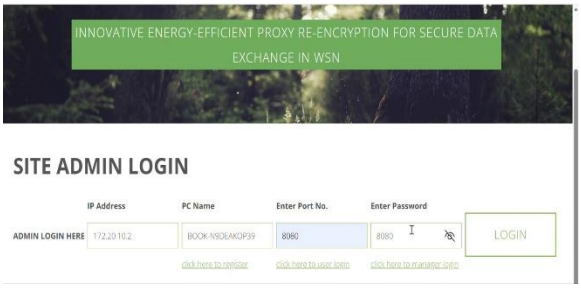


Fig. 5: Site Admin Login

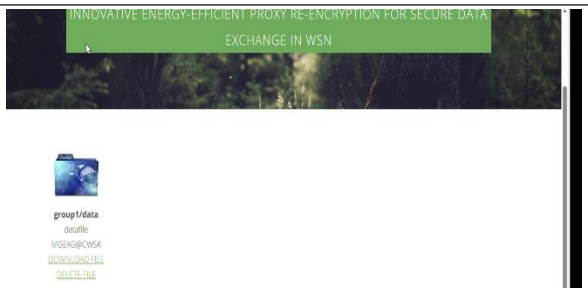


Fig. 6: Group Data

V. CONCLUSION

This paper presented an innovative PRE scheme designed to address the unique challenges encountered in WSNs. The PRE is tailored between CHs to facilitate secure intra- and inter-cluster communication, data sharing, and authentication among WSN nodes. To optimize efficiency and conserve resources, the proposed design is adept in managing the cryptographic computational overhead through a balanced combination of lightweight symmetric and asymmetric encryption techniques. The Speck symmetric encryption was employed to secure the SN data, whereas reencryption relied on ECC to handle the symmetric encryption keys attached to the ciphertext. Moreover, an efficient key management technique was designed to ensure secure key generation, distribution, and freshness in the dynamic WSN environment. The evaluation results robustly validate the efficacy of our tailored PRE scheme in WSNs, demonstrating its ability to significantly enhance encryption,

re-encryption, and decryption performance while minimizing the strain on the constrained resources of SNs. Moreover, our scheme exhibits remarkable scalability, effectively addressing challenges commonly associated with centralized-based PRE approaches. Additionally, by distributing PRE tasks across the WSN, our design adeptly mitigates the risk of a single point of failure, enhancing the overall robustness and reliability of the system. The evaluation results demonstrate a notable 40% reduction in SN power consumption and a 32% decrease in overall network power consumption compared to existing PRE solutions designed for resource-constrained environments. The substantial processing time reduction in our PRE scheme, attributed to lightweight and proxy re-encryption methods, amplifies CH efficiency while maintaining robust security measures. Security analyses confirmed the scheme's proficiency in meeting essential security requirements, including confidentiality, authentication, integrity, and resilience against collusion and repudiation. The proposed scheme exhibits robustness against common WSN threats, such as replay, Sybil, man in-the-middle, and brute-force attacks.

REFERENCES

1. O. A. Khashan, R. Ahmad and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks", Ad Hoc Netw., vol. 115, Apr. 2021.

2. O. A. Khashan, S. Alamri, W. Alomoush, M. K. Alsmadi, S. Atawneh and U. Mir, "Blockchainbased decentralized authentication model for IoT-based E-learning and educational environments", Comput. Mater. Continua, vol. 75, no. 2, pp. 3133-3158, 2023.

3. I. Mashal, O. A. Khashan, M. Hijjawi and M. Alshinwan, "The determinants of reliable smart grid from experts' perspective", Energy Informat., vol. 6, no. 1, pp. 1-23, Apr. 2023.

4. O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems", J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 2, pp. 726-739, Feb. 2023.

5. A. Sufyan, K. B. Khan, O. A. Khashan, T. Mir and U. Mir, "From 5G to beyond 5G: A comprehensive survey of wireless network evolution challenges and

promising technologies", Electronics, vol. 12, no. 10, pp. 2200, May 2023.

6. F. H. El-Fouly, M. Kachout, Y. Alharbi, J. S. Alshudukhi, A. Alanazi and R. A. Ramadan, "Environment-aware energy efficient and reliable routing in real-time multi-sink wireless sensor networks for smart cities applications", Appl. Sci., vol. 13, no. 1, pp. 605, Jan. 2023.

7. Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. Journal of Computer Science and Technology Studies, 7(8), 1097-1104.

8. Garapati, R. S., Aitha, A. R., Yandamuri, U. S., Gottimukkala, V. R. R., Nagubandi, A. R., & Kolla, S. H. (2026, March). Cloud-Native Orchestration of Multi-Counterparty Derivatives and Collateral in Manufacturing Enterprises via AI-Assisted Financial Audit Engines. In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 1-6). IEEE.

AUTHORS Profile



Mrs. ROJARAMANI ADAPA, received M.Tech (CSE) from JNTUH. She has teaching experience 20 yrs and has guided many undergraduate and post graduate projects. She has published about 10 research articles in peer reviewed journals and presented 5 research papers at various National Conferences. At present she is working as Asst. Prof. in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mrs. BADDAM DIMPUL REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GANGONI SAI PAVAN pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. B V THARUN TEJA REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. BACHU BHANU PRASAD pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.