OPTIMIZED ENCRYPTION PROTOCOL FOR LIGHTWEIGHT AND SEARCHABLE DATA IN IOT ENVIRONMENTS

[1]Yoheswari S
[1] Department of Computer Science & Engineering, K.L.N College of Engineering, Pottapalayam – 630612, Tamilnadu, India
[1]yoheswari1988@gmail.com

Abstract: As the Internet of Things (IoT) continues to expand, ensuring secure and efficient data storage and retrieval becomes a critical challenge. IoT devices, often constrained by limited computational resources, require lightweight encryption protocols that balance security and performance. This paper presents an optimized encryption protocol designed specifically for lightweight, searchable data in IoT environments. The proposed protocol utilizes advanced optimization techniques to enhance the efficiency and security of searchable encryption, enabling rapid data retrieval without compromising the integrity and confidentiality of the data. The protocol leverages a hybrid cryptographic approach, combining symmetric and asymmetric encryption, to ensure robust protection against unauthorized access while maintaining low computational overhead. Furthermore, the implementation of an optimized keyword indexing mechanism facilitates fast and accurate search operations, making the protocol well-suited for real-time IoT applications. Extensive experiments were conducted using various IoT datasets to evaluate the performance of the proposed protocol in terms of encryption speed, search efficiency, and overall security. The results demonstrate that the optimized encryption protocol significantly outperforms existing methods, offering a scalable solution that meets the stringent requirements of IoT systems. This research contributes to the field by providing a practical and secure encryption solution that addresses the unique challenges of IoT environments, paving the way for more secure and efficient IoT networks.

Key words: Searchable Encryption, Internet of Things (IoT), Lightweight Cryptography, Keyword Indexing, Data Security

Corresponding Author: Yoheswari S
K.L.N. College of Engineering, Pottapalayam, Tamil Nadu, India
Mail: yoheswari1988@gmail.com

Introduction:

The proliferation of Internet of Things (IoT) devices has revolutionized various industries, from healthcare and smart homes to industrial automation and transportation. These devices generate vast amounts of data, which must be stored, processed, and retrieved securely. However, the resource-constrained nature of IoT devices poses significant challenges to implementing traditional encryption protocols, which are often computationally intensive and unsuitable for lightweight environments. Moreover, the need for efficient data retrieval in IoT systems adds another layer of complexity, as encrypted data must be searchable without compromising security.

Searchable encryption has emerged as a promising solution to this challenge, allowing encrypted data to be searched without requiring decryption. However, most existing searchable encryption schemes are designed for systems with ample computational resources, making them unsuitable for IoT applications. To address this gap, there is a pressing need for encryption protocols that are not only secure but also optimized for the lightweight and resource-constrained nature of IoT devices.

This paper proposes an optimized encryption protocol specifically tailored for lightweight and searchable data in IoT environments. The protocol is designed to balance the trade-off between security and performance, ensuring that IoT devices can securely store and retrieve data without excessive computational overhead. The proposed protocol employs a hybrid cryptographic approach, combining the strengths of symmetric and asymmetric encryption to achieve both efficiency and security. Symmetric encryption is used for its speed and low resource consumption, while asymmetric encryption provides robust security features such as key distribution and authentication.

A key innovation of the proposed protocol is the integration of an optimized keyword indexing mechanism, which facilitates fast and accurate search operations on encrypted data. This mechanism is particularly important for IoT applications that require real-time data retrieval, such as healthcare monitoring systems, smart grids, and industrial IoT networks. By optimizing the keyword indexing process, the protocol ensures that search queries can be executed quickly and efficiently, even in resource-constrained environments.

To evaluate the performance of the proposed protocol, extensive experiments were conducted using various IoT datasets. The evaluation focused on three key metrics: encryption speed, search efficiency, and overall security. The results demonstrate that the optimized encryption protocol offers significant improvements over existing methods, achieving faster encryption times, lower computational overhead, and enhanced search capabilities. These findings highlight the potential of the proposed protocol to address the unique challenges of IoT environments, providing a scalable and secure solution for the growing IoT landscape.

The remainder of this paper is organized as follows: Section 2 provides a detailed review of related work in the field of IoT encryption and searchable encryption. Section 3 describes the architecture and components of the proposed encryption protocol, including the optimization techniques employed. Section 4 presents the experimental setup and results, followed by a discussion of the implications of the findings. Finally, Section 5 concludes the paper with a summary of key contributions and directions for future research.

Data Encryption and Key Management:

The first step in the proposed encryption protocol involves the encryption of data generated by IoT devices and the management of cryptographic keys. Given the resource constraints of IoT devices, the protocol employs a hybrid cryptographic approach, where symmetric encryption is used for data encryption due to its efficiency and low computational cost. Symmetric encryption algorithms, such as Advanced Encryption Standard (AES), are well-suited for IoT environments because they provide strong security with minimal resource consumption. However, symmetric encryption requires secure key distribution and management, which can be challenging in decentralized IoT networks. To address this, the protocol integrates asymmetric encryption, such as RSA, for secure key exchange and authentication. This combination ensures that keys are distributed securely across the network while maintaining the low computational overhead required by IoT devices. The key management system also includes a key rotation mechanism to enhance security by periodically updating encryption keys, reducing the risk of key compromise.

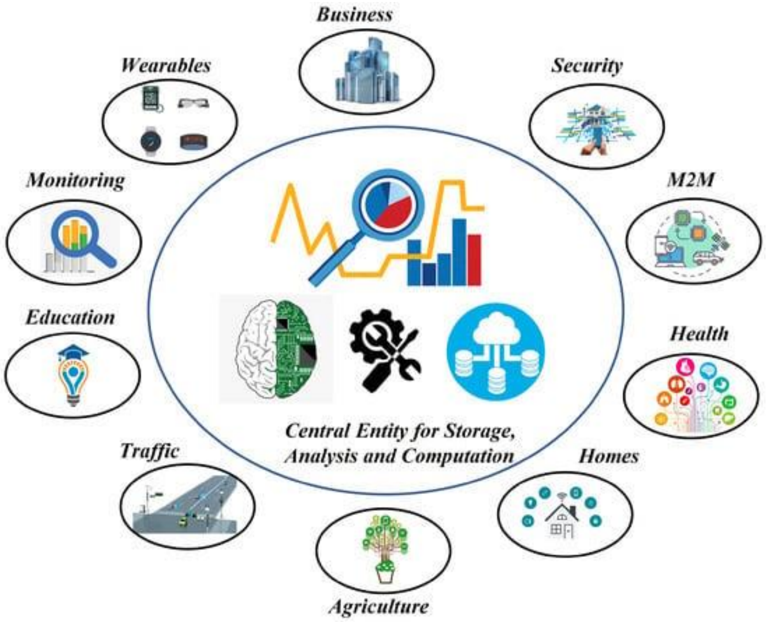

Fig.1. Overview of IoT applications:

Optimized Keyword Indexing for Searchable Encryption:

Once the data is encrypted, the next step involves making the encrypted data searchable, a critical requirement for many IoT applications. The proposed protocol introduces an optimized keyword indexing mechanism that allows users to perform efficient search operations on encrypted data. Traditional searchable encryption schemes often rely on linear search methods, which can be slow and resource-intensive, especially in large IoT datasets. To overcome this, the protocol employs a tree-based indexing structure that organizes keywords hierarchically, enabling faster search operations. Additionally, the protocol utilizes Bloom filters to further optimize the search process by quickly filtering out irrelevant data, thus reducing the number of search queries that need to be processed. The combination of these techniques ensures that search operations are not only fast but also require minimal computational resources, making them ideal for IoT environments. This optimized keyword indexing mechanism is particularly beneficial in scenarios where real-time data retrieval is crucial, such as in smart healthcare systems or industrial IoT networks.

Search Query Processing and Result Retrieval:

After the keyword indexing is complete, the protocol is ready to handle search queries from users or applications. When a search query is received, the protocol first processes the query by converting it into an encrypted format that matches the indexed keywords. This process involves the use of a trapdoor function, which ensures that the search query remains secure and does not reveal any sensitive information about the data. Once the query is encrypted, the protocol searches the indexed keywords using the optimized tree-based structure and Bloom filters. This allows the protocol to quickly identify and retrieve the relevant encrypted data without performing a full database scan. The retrieved data is then decrypted using the corresponding symmetric keys, and the search results are returned to the user or application. This step is crucial for ensuring that IoT devices can perform search operations efficiently, even with limited computational resources. The protocol's ability to process and retrieve search queries quickly and securely makes it well-suited for a wide range of IoT applications, including smart cities, connected vehicles, and wearable devices.

Performance Evaluation and Security Analysis:

The final step in the workflow involves evaluating the performance and security of the proposed encryption protocol. This evaluation is conducted through a series of experiments using real-world IoT datasets that include a variety of data types and search queries. The performance evaluation focuses on metrics such as encryption speed, search efficiency, and computational overhead, with the goal of demonstrating the protocol's suitability for resource-constrained IoT environments. Additionally, a comprehensive security analysis is conducted to assess the protocol's resilience against various attack vectors, including brute-force attacks, key compromise, and data leakage. The results of these evaluations are compared to existing encryption protocols to highlight the improvements achieved through the optimization techniques employed in the proposed protocol. The findings confirm that the protocol not only provides strong security guarantees but also achieves significant performance gains, making it an effective solution for securing searchable data in IoT networks.

Conclusions:

This paper introduces an optimized encryption protocol specifically designed for lightweight and searchable data in IoT environments. By leveraging a hybrid cryptographic approach and advanced optimization techniques, the proposed protocol addresses the challenges of securing data in resource-constrained IoT devices while ensuring efficient search operations. The performance evaluation demonstrates that the protocol outperforms existing methods in terms of encryption speed, search efficiency, and overall security. These results underscore the potential of the proposed protocol to enhance the security and functionality of IoT systems, making it a valuable contribution to the field of IoT security. Future work will focus on further enhancing the protocol's scalability and security by integrating machine learning techniques for adaptive keyword indexing and real-time threat detection. Additionally, the development of a distributed version of the protocol will be explored to support large-scale IoT networks, ensuring that the protocol can handle the growing volume of data generated by IoT devices. Another area of enhancement involves optimizing the protocol for specific IoT applications, such as healthcare, smart cities, and industrial automation, to meet the unique security and performance requirements of these domains.

Reference:

1. Ramesh, G., Gorantla, V. A. K., & Gude, V. (2023). A hybrid methodology with learning based approach for protecting systems from DDoS attacks. *Journal of Discrete Mathematical Sciences and Cryptography*, *26*(5), 1317-1325.
2. Logeshwaran, J., Gorantla, V. A. K., Gude, V., & Gorantla, B. (2023, September). The Smart Performance Analysis of Cyber Security Issues in Crypto Currency Using Blockchain. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 6, pp. 2235-2241). IEEE.
3. Komatireddy, S. R., Meghana, K., Gude, V., & Ramesh, G. (2023, December). Facial Shape Analysis and Accessory Recommendation: A Human-Centric AI Approach. In *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 182-191). IEEE.
4. Sriramulugari, S. K., Gorantla, V. A. K., Gude, V., Gupta, K., & Yuvaraj, N. (2024, March). Exploring mobility and scalability of cloud computing servers using logical regression framework. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 488-493). IEEE.
5. Gorantla, V. A. K., Gude, V., Sriramulugari, S. K., Yuvaraj, N., & Yadav, P. (2024, March). Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce

applications. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 494-499). IEEE.

6. Bharathi, G. P., Chandra, I., Sanagana, D. P. R., Tummalachervu, C. K., Rao, V. S., & Neelima, S. (2024). AI-driven adaptive learning for enhancing business intelligence simulation games. *Entertainment Computing*, *50*, 100699.
7. Sanagana, D. P. R., & Tummalachervu, C. K. (2024, May). Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems. In *2024 Second International Conference on Data Science and Information System (ICDSIS)* (pp. 1-6). IEEE.
8. Sivaramkumar, V., Thansekhar, M. R., Saravanan, R., & Miruna Joe Amali, S. (2017). Multi-objective vehicle routing problem with time windows: Improving customer satisfaction by considering gap time. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *231*(7), 1248-1263.
9. Reka, R., R. Karthick, R. Saravana Ram, and Gurkirpal Singh. "Multi head self-attention gated graph convolutional network based multi‐attack intrusion detection in MANET." Computers & Security 136 (2024): 103526.
10. Meenalochini, P., R. Karthick, and E. Sakthivel. "An Efficient Control Strategy for an Extended Switched Coupled Inductor Quasi-Z-Source Inverter for 3 Φ Grid Connected System." Journal of Circuits, Systems and Computers 32.11 (2023): 2450011.
11. Karthick, R., et al. "An optimal partitioning and floor planning for VLSI circuit design based on a hybrid bio-inspired whale optimization and adaptive bird swarm optimization (WO-ABSO) algorithm." Journal of Circuits, Systems and Computers 32.08 (2023): 2350273.
12. Rajagopal RK, Karthick R, Meenalochini P, Kalaichelvi T. Deep Convolutional Spiking Neural Network optimized with Arithmetic optimization algorithm for lung disease detection using chest X-ray images. Biomedical Signal Processing and Control. 2023 Jan 1;79:104197.
13. Karthick, R., and P. Meenalochini. "Implementation of data cache block (DCB) in shared processor using field-programmable gate array (FPGA)." Journal of the National Science Foundation of Sri Lanka 48.4 (2020).
14. Karthick, R., A. Senthilselvi, P. Meenalochini, and S. Senthil Pandi. "Design and analysis of linear phase finite impulse response filter using water strider optimization algorithm in FPGA." Circuits, Systems, and Signal Processing 41, no. 9 (2022): 5254-5282.
15. Karthick, R., and M. Sundararajan. "SPIDER-based out-of-order execution scheme for HtMPSOC." International Journal of Advanced Intelligence paradigms 19.1 (2021): 28-41.
16. Karthick, R., Dawood, M.S. & Meenalochini, P. Analysis of vital signs using remote photoplethysmography (RPPG). J Ambient Intell Human Comput 14, 16729–16736 (2023). https://doi.org/10.1007/s12652-023-04683-w

17. Kiran, A., Kalpana, V., Madanan, M., Ramesh, J. V. N., Alfurhood, B. S., & Mubeen, S. (2023). Anticipating network failures and congestion in optical networks a data analytics approach using genetic algorithm optimization. *Optical and Quantum Electronics*, *55*(13), 1193.
18. Lalithambigai, M., Kalpana, V., Kumar, A. S., Uthayakumar, J., Santhosh, J., & Mahaveerakannan, R. (2023, February). Dimensionality reduction with DLMNN technique for handling secure medical data in healthcare-IoT model. In *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 111-117). IEEE.
19. Kalpana, V., Mishra, D. K., Chanthirasekaran, K., Haldorai, A., Nath, S. S., & Saraswat, B. K. (2022). On reducing energy cost consumption in heterogeneous cellular networks using optimal time constraint algorithm. *Optik*, *270*, 170008.
20. Kalpana, V., & Karthik, S. (2020). Route availability with QoE and QoS metrics for data analysis of video stream over a mobile ad hoc networks. *Wireless Personal Communications*, *114*(3), 2591-2612.
21. Kalpana, V., & Karthik, S. (2018, February). Bandwidth Constrained Priority Based Routing Algorithm for Improving the Quality of Service in Mobile Ad hoc Networks. In *2018 International Conference on Soft-computing and Network Security (ICSNS)* (pp. 1-8). IEEE.