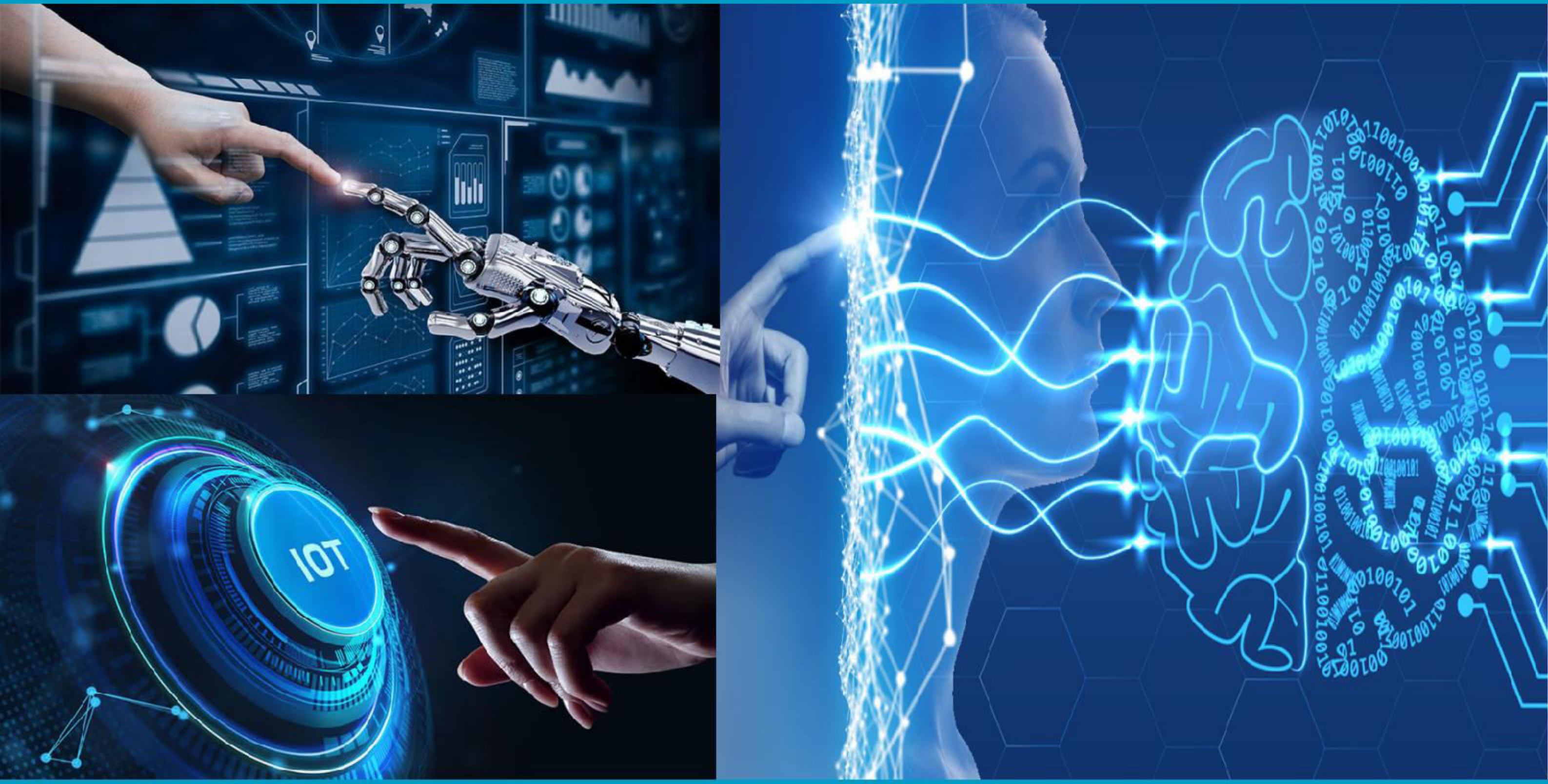
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 11, Issue 11, November 2024

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.802

Secure Communication Frameworks for Fog Systems: A Cryptographic Approach

R. Nivethitha[1]*, R. Vanitha Mani [2], Dr.D.Rajinigirinath[3]

PG Student, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, Tamil Nadu, India[1]

Assistant Professor, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, Tamil Nadu, India[2]

Professor, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, Tamil Nadu, India[3]

ABSTRACT: Fog computing extends cloud capabilities to the edge of the network, providing real-time data processing with low latency. However, the decentralized structure of fog nodes introduces significant security concerns, especially in establishing secure communication channels. In this paper, we propose an Efficient Fog Node Authentication and Key Exchange (EFNAKE) protocol designed to enhance secure communication in fog environments. The EFNAKE protocol enables fog nodes to authenticate each other and exchange cryptographic keys securely, without relying on a centralized authority. This scheme ensures mutual authentication, data integrity, and confidentiality, making it suitable for dynamic and resource-constrained environments. It also supports scalable communication and provides resilience against potential attacks, ensuring the robustness of fog-based applications such as IoT, smart cities, and industrial automation..

KEYWORDS: Fog Node Authentication, Key Exchange, Secure Communication, Data Integrity, Mutual Authentication, Fog-based Applications.

I. INTRODUCTION

Centralized cloud computing systems often fall short in meeting the needs of applications that demand low latency and quick response times. Challenges like limited network capacity and the physical distance between servers and users make it difficult to support the rapid growth of connected devices. A new paradigm is required to overcome these limitations.

Fog computing addresses these issues by shifting data processing to the network edge, closer to users. This approach reduces delays, enhances service quality, and supports diverse applications, including smart cities, industrial systems, and IoT devices, offering a more seamless user experience.

The distributed nature of fog systems, however, raises security concerns, especially for communication between nodes. This paper introduces a Dynamic Contributory Broadcast Encryption (DConBE) method, providing a secure and scalable solution for fog environments, enabling reliable communication without the need for a centralized authority.

II. EXISTING SYSTEM

Fog systems today are primarily designed for secure communication and data processing at the edge, yet they struggle with scalability and adaptability.:

- The complexity of communication and computation increases in large fog systems, where nodes frequently join and leave the network.
- Dynamic changes in fog nodes demand flexible and effective key management to maintain secure communication.
- Contributory Broadcast Encryption (ConBE) allows fog nodes to collectively generate a public encryption key while keeping individual decryption keys private.
- Users can send encrypted messages to selected fog nodes using the shared public encryption key, ensuring secure communication.
- If a Private Key Generator (PKG) is compromised, it threatens all messages associated with that key pair, making key updates necessary to mitigate security risks.

III. PROPOSED SYSTEM

The proposed system addresses the limitations of current fog computing models by utilizing Dynamic Contributory Broadcast Encryption (DConBE) for secure and efficient key management. Key features include:

- Enabling fog nodes to collaboratively generate public encryption keys and individual decryption keys in a single round, without the need for a trusted third party.
- Allowing fog nodes to join or leave the system dynamically while maintaining a secure communication environment.
- Solving the challenge of encrypted data deduplication through the use of cryptographic puzzles to enhance data security in fog systems.
- Introducing efficient key management solutions that ensure consistent and reliable communication across fog nodes.
- Providing theoretical security proofs and experimental results to demonstrate the practicality and effectiveness of the proposed key management system.

IV. ARCHITECTURE DIAGRAM

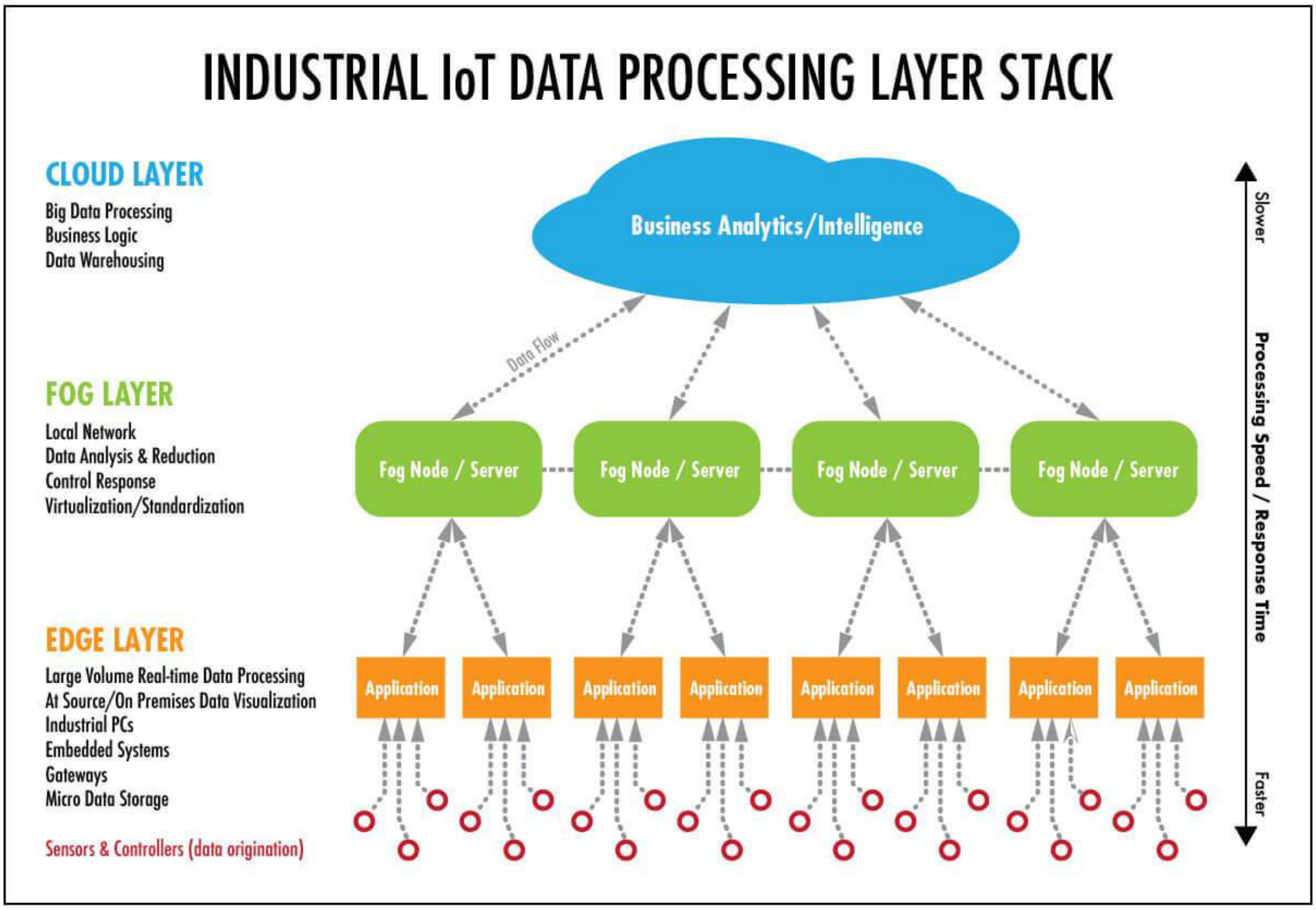

INDUSTRIAL IoT DATA PROCESSING LAYER STACK
CLOUD LAYER
Big Data Processing
Business Logic
Data Warehousing
Business Analytics/Intelligence
Data Flow
FOG LAYER
Local Network
Data Analysis & Reduction
Control Response
Virtualization/Standardization
Fog Node / Server
Fog Node / Server
Fog Node / Server
Fog Node / Server
EDGE LAYER
Large Volume Real-time Data Processing
At Source/On Premises Data Visualization
Industrial PCs
Embedded Systems
Gateways
Micro Data Storage
Application
Sensors & Controllers (data origination)
Slower
Processing Speed / Response Time
Faster

Fig 4.1. Architecture Diagram

A.ARCHITECTURE EXPLANATION

The **Industrial IoT Data Processing Layer Stack** is a structured architecture designed to optimize data handling and decision-making in industrial environments by dividing tasks into three layers: the **Edge Layer**, **Fog Layer**, and **Cloud Layer**. The **Edge Layer** is the foundation where data originates, leveraging sensors and controllers to collect real-time data. This layer processes large volumes of data locally using embedded systems, gateways, industrial PCs, and micro data storage. By performing real-time processing and visualization at the source, it minimizes latency and ensures rapid response for critical applications, such as predictive maintenance and immediate fault detection.

The **Fog Layer** serves as the intermediate processing layer, bridging the Edge and Cloud Layers. It aggregates data from multiple edge devices, reduces redundancy through local preprocessing, and supports standardization and virtualization for seamless data management. Fog nodes or servers in this layer provide additional functionality like control response, enabling localized decision-making without overburdening the cloud. This layer helps to optimize network bandwidth by filtering and summarizing data, ensuring that only relevant information reaches the cloud, thereby improving system scalability and efficiency.

The **Cloud Layer** is the centralized hub for big data processing, business analytics, and data warehousing. It supports complex computations, long-term storage, and high-level analysis to generate actionable insights for decision-makers. Advanced machine learning models and AI-driven analytics are often implemented in this layer to enhance predictive capabilities and strategic planning. Data flows upward from the Edge to the Fog and finally to the Cloud, ensuring a seamless processing pipeline. This layered architecture enhances reliability, reduces latency, and supports real-time and long-term decision-making, making it vital for modern Industrial IoT systems.

Additionally, this stack offers flexibility and adaptability, as tasks can be dynamically distributed among layers depending on network conditions, system demands, and application requirements. By decentralizing certain operations to the Fog and Edge Layers, it reduces dependency on cloud connectivity, ensuring uninterrupted performance even in environments with limited internet access. Furthermore, the architecture supports security enhancements, as sensitive data can be processed locally in the Edge and Fog Layers, reducing the risk of breaches during transmission to the cloud. This approach is increasingly adopted in industries such as manufacturing, agriculture, healthcare, and smart cities to meet the growing demand for precision, scalability, and efficiency in IoT-driven systems.

V. MODULES

A. Administrator Dashboard

The Administrator Dashboard serves as the central access point to the system. This module is designed to authenticate users through a secure login process where valid credentials (username and password) are required. If the entered information does not match the system's records, the login attempt is denied, safeguarding the system against unauthorized users. Only verified users are granted access to manage the system and assign tasks. The administrator can configure and monitor system activities, ensuring that all operations are conducted securely. This module strengthens the overall security of the system by ensuring only authorized personnel can interact with sensitive areas of the platform.

B. Node Control Interface

The Node Control Interface is responsible for managing the interaction between the admin and the network of nodes. Upon successful login, the admin is able to assign specific roles or tasks to each node in the system. This module allows nodes to execute their respective tasks autonomously while remaining under the supervision of the admin. Once the tasks are completed, each node securely uploads the processed files to the database. The node interface is designed to streamline communication between multiple nodes, allowing efficient task delegation and progress tracking. It plays a vital role in coordinating node activities, ensuring that all nodes are working as expected within the system.

C. File Upload and Encryption

The File Upload and Encryption module is designed to securely upload files to the system's central storage. Each node, upon completing its designated task, encrypts the data before uploading it to the database. This encryption ensures that any sensitive information remains protected during transit and while stored. The module also handles the organization of encrypted files, maintaining the integrity of the data with necessary metadata for later retrieval. This system ensures that unauthorized users cannot access the files, as they remain encrypted at all stages. By using advanced encryption techniques, this module ensures that the files are protected throughout the entire process, from upload to storage**.**

D. File Access Request Management

The File Access Request Management module controls the process through which nodes request access to files uploaded by other nodes. If a node wishes to access a particular file, it must send a formal request to the node who uploaded the file. This request is reviewed, and the uploader node either grants or denies access. This mechanism ensures that files are only shared with authorized nodes, maintaining security throughout the file-sharing process. Requests and responses are securely managed and logged for transparency. The module plays an essential role in ensuring that file access is controlled and that files are only shared between trusted nodes**.**

E. Access Granting and Denial

The Access Granting and Denial module governs the approval process for file access requests. Once a node submits a request to access a file, the owner of the file (the uploader node) reviews the request and either approves or denies it. If approved, the requesting node is allowed to access the file; if denied, the request is rejected, and the file remains inaccessible. This module ensures that files are not shared improperly and only authorized entities can view them. It is crucial for maintaining the integrity of the system by enforcing strict file access control. Each request and response is handled securely, preventing unauthorized access to sensitive data.

F. Key Generation and File Download

The Key Generation and File Download module is responsible for providing the correct decryption keys to nodes after receiving access approval. Once a node is granted access, the admin generates a unique decryption key for the requested file and sends it securely to the requesting node. The node then uses this key to decrypt the file and download the original content. If an incorrect key is entered, the download is blocked to prevent unauthorized access. This module ensures that only nodes with the correct decryption keys can access the sensitive files. It adds a final layer of security to the system, ensuring that downloaded files remain protected and are only accessible by authorized parties.

VI. CONCLUSION

In conclusion, we have presented an innovative key management framework for fog computing based on Efficient Fog Node Authentication and Key Exchange (EFNAKE). This framework allows end users to securely send encrypted messages to selected fog nodes without relying on a trusted third party. The EFNAKE scheme efficiently supports the dynamic nature of fog environments, enabling fog nodes to join or leave the system with minimal overhead. The security of our proposed method has been validated under the decision BDHE assumption in the standard model, ensuring its robustness. A notable strength of EFNAKE is its ability to manage dynamic node participation while maintaining strong security guarantees. However, the current approach requires users to be aware of the fog node structure in advance. Future work could focus on developing an EFNAKE-based solution that does not rely on prior knowledge of the fog node structure, further enhancing scalability and flexibility in highly dynamic fog computing systems.

REFERENCES

1. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and Z. Dong, “Roundefficient and sender-unrestricted dynamic group key agreement protocol for secure group communications,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2352–2364, Nov. 2015. ZHANG: KEY MANAGEMENT SCHEME FOR SECURE CHANNEL ESTABLISHMENT IN FOG COMPUTING 1127
2. InterPlanetary file system. [Online]. Available: https://ipfs.io/, Accessed on:12 Mar. 2019.
3. “Multiprecision integer and rational arithmetic,” C++ Library (MIRACL). [Online]. Available: https://miracl.com/
4. Q. Pei, B. Kang, L. Zhang, K. Choo, Y. Zhang, and Y. Sun, “Secure and privacy-preserving 3D vehicle positioning schemes for vehicular ad hoc network,” EURASIP J. Wireless Commun. Netw., vol. 2018, p. 271, Dec. 2018.
5. R. Canetti, S. Halevi, and J. Katz, “Chosen-ciphertext security from identity-based encryption,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2004, pp. 207–222.
6. W. Liu, J. Liu, Q. Wu, B. Qin, and Y. Zhou, “Practical direct chosen ciphertext secure key-policy attribute-based encryption with public ciphertext test,” in Proc. Eur. Symp. Res. Comput. Secur., 2014, pp. 91–108.
7. T. Matsuda and G. Hanaoka, “Chosen ciphertext security via UCE,” in Proc. Int. Conf. Practice Theory Public-Key Cryptography, 2014, pp. 56–76.
8. C. Gentry and B. Waters, “Adaptive security in broadcast encryption systems (with short ciphertexts),” in Proc. 28th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2009, pp. 171–188.
9. D. Boneh, X. Boyen, and E. Goh, “Hierarchical identity based encryption with constant size ciphertext,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.
10. Y. Guo, Z. Zhang, and Y. Guo, “SecFHome: Secure remote authentication in fog-enabled smart home environment,” Comput. Netw., vol. 207, Apr. 2022, Art. no. 108818.
11. S. O. Ogundoyin and I. A. Kamil, “Secure and privacy-preserving D2D communication in fog computing services,” Comput. Netw., vol. 210, Jun. 2022, Art. no. 108942.
12. S. Feng, P. Setoodeh, and S. Haykin, “Smart home: Cognitive interactive people-centric Internet of Things,” IEEE Commun. Mag., vol. 55, no. 2, pp. 34–39, Feb. 2017.
13. S. A. Ahmed, “A performance study of hyperledger fabric in a smart home and IoT environment,” M.S. thesis, Dept. Inform., Fac. Math. Natural Sci., Univ. Oslo, Oslo, Norway, 2019.
14. M. Rahimi, M. Songhorabadi, and M. H. Kashani, “Fog-based smart homes: A systematic review,” J. Netw. Comput. Appl., vol. 153, Mar. 2020, Art. no. 102531.
15. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, Feb. 2014.

INNO SPACE
SJIF Scientific Journal Impact Factor

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

☎ +91 99405 72462 ☎ +91 63819 07438 ✉ ijmrsetm@gmail.com

www.ijmrsetm.com