IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311203|

Revolutionizing Edge Security: Adaptive Key Management in Fog Computing

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

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

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

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

ABSTRACT: Fog computing brings computation closer to the edge of the network, improving performance and reducing latency for real-time applications. However, the decentralized nature of fog nodes creates significant security challenges, particularly in ensuring secure communication and key management. To address these challenges, we propose a novel Distributed Key Agreement Scheme (DKAS) for secure communication within fog environments. This scheme enables fog nodes to autonomously generate and share encryption keys without relying on a central authority, allowing efficient encryption and decryption of messages. Additionally, the scheme supports dynamic node participation, ensuring scalability and flexibility in highly dynamic fog networks. Our approach enhances security by preventing unauthorized access, ensuring data confidentiality, and maintaining key integrity across the system. This solution is well-suited for IoT and smart device networks, where low latency and secure communication are paramount.

KEYWORDS: Distributed Key Agreement, Fog Computing, Secure Communication,Key Management, IoT Security, Dynamic Node Participation.

I. INTRODUCTION

As connected devices grow exponentially, traditional cloud computing struggles to support latency-sensitive applications due to limited bandwidth and the long distance between users and centralized servers. This highlights the need for a new computing model to deliver efficient and responsive services.

Fog computing extends cloud capabilities by enabling data processing at the network edge, closer to end-users. This reduces latency, improves Quality of Service (QoS), and supports a variety of real-time applications, such as smart transportation, industrial automation, and IoT-based systems.

Despite its benefits, the decentralized architecture of fog nodes introduces significant security challenges. To address this, we propose a Dynamic Contributory Broadcast Encryption (DConBE) framework, which ensures secure and scalable communication in fog networks without relying on centralized entities, promoting adaptability and resilience.

II. EXISTING SYSTEM

The current fog computing systems mainly concentrate on key management and encryption protocols, but they face several challenges**:**

- Large fog networks experience increased communication and computational complexity due to the constant change in node participation.
- The dynamic addition and removal of fog nodes necessitate continuous updates to key management strategies for ensuring system security.
- Contributory Broadcast Encryption (ConBE) allows fog nodes to collaboratively generate an encryption key while maintaining individual decryption keys for secure communication.
- End users can encrypt messages using the public key and send them securely to specific fog nodes within the system.
- If the Private Key Generator (PKG) is compromised, all messages using that key pair are vulnerable, requiring regular key updates to protect the system's integrity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311203|

III. PROPOSED SYSTEM

The proposed system overcomes the limitations of existing fog computing models by leveraging Dynamic Contributory Broadcast Encryption (DConBE) for secure key exchange and communication. Key features include:

- Allowing fog nodes to generate and exchange encryption keys collaboratively, eliminating the need for a trusted third party.
- Enabling dynamic node participation, where fog nodes can securely join or leave the system without compromising security.
- Addressing encrypted data deduplication by using cryptographic puzzles, ensuring secure handling of data in fog environments.
- Providing a robust key management solution to establish and maintain secure communication channels across diverse fog nodes.
- Offering thorough security proofs and real-world experimental validation, demonstrating the scalability and effectiveness of the proposed system.

IV. ARCHITECTURE DIAGRAM

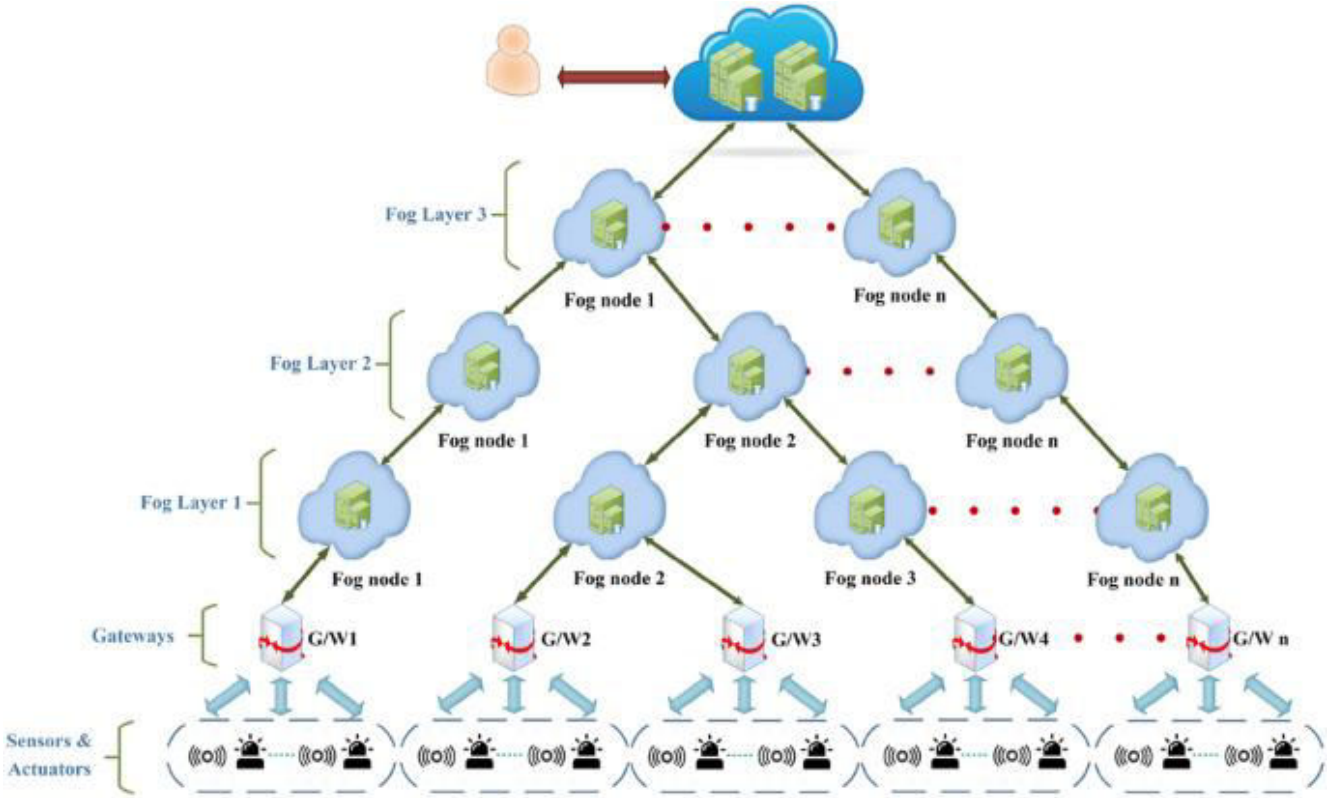

Fig 4.1. Architecture Diagram

A.ARCHITECTURE EXPLANATION

The Fog Computing Architecture in Industrial IoT provides a layered approach to optimize data processing, decision-making, and communication by leveraging a hierarchical framework of sensors, gateways, fog nodes, and cloud infrastructure. At the base, Sensors and Actuators generate raw data and execute control commands in real-time. These devices transmit data to Gateways, which aggregate, filter, and preprocess the data, ensuring efficient communication with the next layer while minimizing unnecessary data flow. The Fog Layer is further divided into sub-layers. The first fog layer directly processes data from gateways, providing low-latency responses, temporary storage, and localized decision-making. The second fog layer coordinates data from multiple first-layer nodes, enabling more complex analytics and ensuring load balancing across the network. The third fog layer serves as a bridge to the Cloud Layer,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311203|

performing high-level aggregation, advanced data analytics, and preparing data for centralized processing. The Cloud Layer, at the top, provides extensive data warehousing, machine learning, and predictive analytics capabilities, supporting long-term strategic decision-making and user-level interaction.

This architecture provides numerous benefits. By processing data locally in the fog layers, it reduces latency and improves real-time responsiveness for critical applications such as predictive maintenance or emergency shutdowns. The hierarchical structure optimizes bandwidth by filtering and summarizing data before transmitting it to higher layers, reducing network congestion. It also enhances reliability since localized processing in fog nodes ensures uninterrupted functionality even if cloud connectivity is disrupted. Scalability is another key feature, as additional fog nodes and layers can be seamlessly integrated to accommodate growing system demands. Security is significantly improved by processing sensitive data at the edge or within fog nodes, minimizing exposure during cloud transmission. Furthermore, the modular nature of this architecture allows customization to meet diverse application needs, including smart manufacturing, healthcare, autonomous systems, and smart cities. The ability to dynamically allocate tasks across layers based on network conditions and application requirements ensures optimal performance and cost efficiency. This distributed yet coordinated approach makes it a robust and future-proof solution for modern Industrial IoT applications.

In addition to its core functionality, the **Fog Computing Architecture** also promotes energy efficiency and sustainability in Industrial IoT systems. By processing data closer to the source in the fog and edge layers, the architecture reduces the power consumption typically associated with transmitting large volumes of raw data to the cloud. Localized processing ensures that only meaningful, processed data is sent to higher layers, significantly reducing the workload on cloud servers and overall energy usage. Moreover, this architecture enhances fault tolerance by allowing individual fog nodes to take over processing tasks if a nearby node fails, ensuring seamless system operation. It also supports heterogeneous device integration, enabling the architecture to accommodate various sensors, protocols, and devices in a single cohesive system. The decentralized nature of fog computing fosters greater autonomy for remote and resource-constrained environments, making it ideal for scenarios like agricultural monitoring, remote healthcare, or industrial automation in areas with limited connectivity. Additionally, the architecture supports real-time updates and dynamic reconfiguration, allowing for on-the-fly adjustments to system requirements, further enhancing its adaptability and operational efficiency. This flexibility positions the fog computing model as a pivotal enabler of next-generation IoT systems that require responsiveness, scalability, and sustainability.

V. MODULES

A. Admin Control Panel

The Admin Control Panel is the starting point for system management, where the administrator logs in using valid credentials. The login module ensures that only legitimate users are permitted to access the system by verifying their username and password. If the credentials do not match, access is denied, preventing unauthorized users from entering the system. This layer of authentication is essential for maintaining the security of the platform. Once authenticated, the admin is granted access to manage all aspects of the system. This module is crucial for user access control and ensuring that only authorized individuals can interact with sensitive data.

B. Node Management Interface

The Node Management Interface allows administrators to allocate tasks to individual nodes after successful login. After logging in, the admin assigns tasks to a set of nodes, which work independently while being overseen by the central control. These nodes are responsible for executing their tasks and subsequently uploading the results to the central database. Each node performs specific duties as per the admin's assignment, ensuring the system's operations run smoothly. This interface is key in organizing and controlling the nodes, making sure all work is distributed effectively across the network of nodes.

C. Encrypted File Upload

The Encrypted File Upload module facilitates the secure transmission of data to the central storage. After completing their designated tasks, nodes encrypt the files before uploading them to the database, ensuring that the data remains secure throughout the process. This encryption prevents unauthorized access, safeguarding the data from any potential threats. The system ensures that files are uploaded in a structured and encrypted format, making them accessible only by users with proper decryption keys. This module plays a crucial role in data security by ensuring that all files are securely encrypted before being stored in the database.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311203|

D. File Access Request Process

The File Access Request Process manages the requests made by nodes that wish to access files stored by other nodes. When a node wants to view or use a file uploaded by another, it must first send a request to the relevant node. The node that uploaded the file then reviews the request and decides whether or not to grant access. This process ensures that sensitive files are only accessible to authorized nodes and prevents any unauthorized sharing. The request process is critical in maintaining a secure file-sharing environment within the system. It ensures that only approved nodes can retrieve files from the database.

E. File Access Approval or Denial

The File Access Approval or Denial module is responsible for handling the responses to file access requests. When a node sends a request to access a file, the file owner evaluates the request and either grants or denies permission to access the file. If the request is approved, the node is permitted to retrieve the file; if rejected, access is denied. This system of access control ensures that only legitimate requests are fulfilled and unauthorized access is prevented. The approval and denial actions are logged and monitored to maintain security and transparency. This module enforces the integrity of the system by ensuring that files are only shared with trusted nodes.

F.. Key Distribution and Secure File Download

The Key Distribution and Secure File Download module is responsible for providing access to encrypted files by distributing the correct decryption keys. Once a node's access request is approved, the admin generates a unique decryption key for that specific file. This key is securely sent to the requesting node, which uses it to decrypt and download the original file. If the wrong key is entered, the file cannot be decrypted, ensuring that unauthorized access is prevented. This module is essential for maintaining the security of the downloaded files, guaranteeing that only the authorized nodes can retrieve and decrypt the content.

VI. CONCLUSION

In conclusion, we have introduced an advanced key management framework for fog computing based on the Distributed Key Agreement Scheme (DKAS). This scheme enables end users to securely send encrypted messages to selected fog nodes without relying on a trusted third party. The DKAS framework efficiently accommodates the dynamic nature of fog environments, allowing fog nodes to join or leave the system with minimal disruption. The security of our proposed method has been demonstrated under the decision BDHE assumption in the standard model, ensuring its reliability. One of the key advantages of DKAS is its ability to manage dynamic node participation while maintaining robust security. However, the current approach requires users to have prior knowledge of the fog node structure. Future work could focus on developing a DKAS-based solution that eliminates the need for such structural knowledge, further improving scalability and adaptability in evolving fog computing systems.

REFERENCES

1. B.Alohali, M. Merabti, and K. Kifayat, "A secure scheme for a smart house based on cloud of things (CoT)," in Proc. 6th Comput. Sci. Electron. Eng. Conf. (CEEC), Sep. 2014, pp. 115–120.
2. M. Amadeo, A. Molinaro, S. Y. Paratore, A. Altomare, A. Giordano, and C. Mastroianni, "A cloud of things framework for smart home services based on information centric networking," in Proc. IEEE 14th Int. Conf. Netw., Sens. Control (ICNSC), May 2017, pp. 245–250.
3. M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet Things J., vol. 3, no. 6, pp. 854–864, Dec. 2016.
4. Y. Guo and Y. Guo, "FogHA: An efficient handover authentication for mobile devices in fog computing," Comput. Secur., vol. 108, Sep. 2021, Art. no. 102358.
5. Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," Comput. Netw., vol. 185, Feb. 2021, Art. no. 107731.
6. Y. Lin, X. Wang, Q. Gan, and M. Yao, "A secure cross-domain authentication scheme with perfect forward security and complete anonymity in fog computing," J. Inf. Secur. Appl., vol. 63, Dec. 2021, Art. no. 103022.
7. M. Amadeo, A. Giordano, C. Mastroianni, and A. Molinaro, "On the integration of information centric networking and fog computing for smart home services," in The Internet Things for Smart Urban Ecosystems. Springer, 2019, pp. 75–93.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311203|

8. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. MCC workshop Mobile cloud Comput., Aug. 2012, pp. 13–16.
9. I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," Concurrency Comput., Pract. Exper., vol. 28, no. 10, pp. 2991–3005, Jul. 2016.
10. S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in Proc. 10th Int. Conf. Wireless Algorithms Syst. Appl. Cham, Switzerland: Springer, 2015, pp. 685–695.
11. J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.
12. Y. Imine, D. E. Kouicem, A. Bouabdallah, and L. Ahmed, "MASFOG: An efficient mutual authentication scheme for fog computing architecture," in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), Aug. 2018, pp. 608–613.
13. B. Huang, X. Cheng, Y. Cao, and L. Zhang, "Lightweight hardware based secure authentication scheme for fog computing," in Proc. IEEE/ACM Symp. Edge Comput. (SEC), Oct. 2018, pp. 433–439.
14. F. M. Salem, "A secure privacy-preserving mutual authentication scheme for publish-subscribe fog computing," in Proc. 14th Int. Comput. Eng. Conf. (ICENCO), Dec. 2018, pp. 213–218.
15. M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," Future Gener. Comput. Syst., vol. 91, pp. 475–492, Feb. 2019.
16. F. Dewanta and M. Mambo, "A mutual authentication scheme for secure fog computing service handover in vehicular network environment," IEEE Access, vol. 7, pp. 103095–103114, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details