IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106021

Enhancing Security in Fog Computing: Dynamic Encryption Protocols for Decentralized Networks

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: As fog computing brings computational resources closer to the data source, it enables faster processing and reduced latency for time-sensitive applications. However, the distributed nature of fog nodes raises significant security concerns, particularly in ensuring the confidentiality and integrity of data transmitted across the network. This paper introduces a novel Secure Group Key Management (SGKM) framework tailored for fog computing environments. The SGKM framework allows fog nodes to dynamically establish and maintain a secure group communication channel through a collaborative key management process. By utilizing lightweight cryptographic techniques, the scheme ensures secure message transmission among fog nodes without relying on a central authority. Additionally, SGKM provides resilience against potential security threats, including node compromise and eavesdropping, making it an ideal solution for applications in IoT and smart networks that require both security and efficiency..

KEYWORDS: Group Key Management, Fog Computing, Secure Communication, Cryptographic Techniques, IoT Security, Data Integrity.

I. INTRODUCTION

Traditional cloud computing struggles to meet the growing demands of modern applications that require low latency and high efficiency. Limited bandwidth and the distance between centralized servers and users hinder its performance for real-time needs. To address these challenges, a new computing approach is essential.

Fog computing pushes computation closer to end-users by utilizing network edge resources, significantly reducing latency and enhancing performance. This approach improves Quality of Service (QoS) and supports a wide range of applications, such as smart transportation, industrial automation, and IoT ecosystems.

However, the decentralized structure of fog nodes poses security challenges, especially in establishing reliable communication. To address this, the study presents a Dynamic Contributory Broadcast Encryption (DConBE) scheme, which ensures secure, adaptable, and scalable communication in fog environments without relying on a centralized trust model.

II. EXISTING SYSTEM

Existing fog computing solutions emphasize secure key exchanges but often fall short in addressing dynamic node management and system resilience:

- In large, collaborative fog networks, communication and computation face challenges due to the dynamic joining and leaving of nodes.
- As fog nodes frequently enter and exit the system, key management schemes must be adaptable to ensure continued security.
- Contributory Broadcast Encryption (ConBE) enables fog nodes to collaboratively establish an encryption key while each node maintains its own decryption key.
- End users can securely send messages to selected fog nodes using the public encryption key, ensuring privacy.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106021

- If the Private Key Generator (PKG) is compromised, all messages encrypted with that key pair are vulnerable, requiring regular updates to the keys to prevent security breaches.

III. PROPOSED SYSTEM

The proposed system overcomes the limitations of existing fog computing frameworks by implementing Dynamic Contributory Broadcast Encryption (DConBE) for secure and scalable key management. Key features include:

- Allowing fog nodes to independently negotiate a shared public encryption key and individual decryption keys without a trusted dealer.
- Supporting dynamic membership, where fog nodes can securely join or leave the system without disrupting ongoing communication.
- Addressing encrypted data deduplication challenges by integrating cryptographic puzzles to ensure data security and privacy.
- Providing an efficient key management framework to establish reliable and secure communication channels across fog nodes.
- Offering comprehensive security proofs and experimental validation to ensure the practicality and robustness of the proposed system in real-world deployments.

IV. ARCHITECTURE DIAGRAM

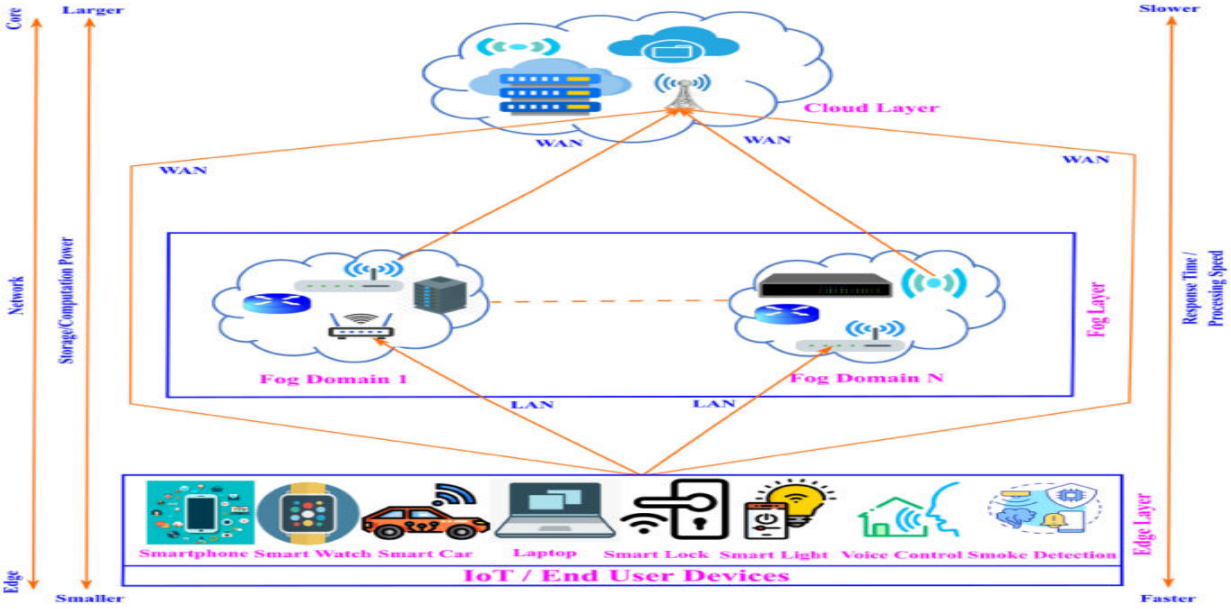

Fig 4.1. Architecture Diagram

A. ARCHITECTURE EXPLANATION

This architecture is designed to handle the increasing volume and complexity of data generated by Internet of Things (IoT) devices and other edge devices. It aims to bring computation and storage closer to the data source, reducing latency and improving efficiency.

Layers:

Cloud Layer:

- Located at the top of the hierarchy, representing centralized cloud computing resources.
- Handles massive data processing, storage, and mining tasks.
- Offers high computing power, reliability, and data storage capacity.

Fog Layer:

- Sits between the cloud and end devices, acting as an intermediary layer.
- Responsible for real-time data processing, analytics, and knowledge discovery.
- Provides storage and processing capabilities closer to the data source, reducing latency.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106021

- Enables location awareness, interactive mobility, and supports devices with limited processing capabilities.
- Divided into multiple Fog Domains, each serving a specific geographical area or set of devices.

End Devices Layer:

- Consists of various IoT devices and other edge devices.
- Generates data and may perform some basic data processing and human interface tasks.
- Leverages the fog layer and cloud layer for more complex processing and storage.

Data Flow:

- Data generated by end devices is initially processed at the fog layer within the respective Fog Domain.
- If further processing or storage is required, the data can be offloaded to the cloud layer or another Fog Domain.
- Results or insights generated in the cloud or fog layer can be sent back to the end devices for decision-making or further actions..

V. MODULES

A. Administrator Control Panel

The Administrator Control Panel module serves as the gateway to the system, where users must authenticate themselves with their credentials (username and password). Only legitimate users with correct login information are allowed access to the main system interface. If the credentials entered are invalid, an error message is shown, ensuring that unauthorized users cannot proceed. Once logged in, the admin has full control over the system, including assigning tasks to nodes and managing permissions. This module guarantees that sensitive actions, such as node configuration and file encryption, are only carried out by authorized personnel. It maintains the overall security by verifying the identity of users and granting necessary access only.

B. Node Management Interface

The Node Management Interface module allows seamless communication between the admin and the nodes after successful login. Each node is assigned specific tasks by the administrator, and the module ensures that nodes can execute their respective duties autonomously while maintaining a structured connection with the admin. After task completion, nodes upload files to the system's database, where they are safely stored and processed. This module ensures proper coordination of tasks and file uploads across multiple nodes, streamlining the overall operation. The interface also manages node statuses and provides real-time updates to the admin, helping track progress. This module ensures that all nodes interact efficiently within the system, ensuring smooth operations.

C. Secure File Upload and Encryption

The Secure File Upload and Encryption module ensures that files are uploaded securely to the system. Once a node finishes its task, it encrypts the file before uploading it to the database, ensuring that sensitive information is protected throughout the process. The encrypted files are stored in the system's database, preventing unauthorized access. This module also organizes the encrypted files with metadata for easy identification and retrieval. It guarantees that files are encrypted during both transmission and storage, making them inaccessible without proper authorization. This layer of encryption ensures that the system adheres to security best practices and prevents data breaches. The Secure File Upload and Encryption module plays a vital role in safeguarding the confidentiality and integrity of data.

D. File Access Request System

File Access Request System module governs the process through which one node can request access to files uploaded by other nodes. If a node wishes to retrieve a file stored by another, it must send a formal request for permission to access the file. The system ensures that access is only granted if the appropriate nodes (both the uploader and the admin) approve the request. This step adds an additional layer of security, ensuring that files are only accessed by authorized entities. All requests are carefully logged to maintain a record of who requested access and for which files. The system ensures that no node can access any file without explicit authorization, promoting secure data sharing.

E. Access Authorization Response

The Access Authorization Response module processes the responses to access requests. Once a node sends a request to access a file, the uploader node reviews the request and either approves or denies it. If approved, access is granted, and the requesting node can proceed to retrieve the file. If denied, the request is rejected, and no further action is taken. This system ensures that files are not shared inappropriately and that only authorized users can access them. Responses are transmitted securely to prevent any interception or alteration. This module maintains tight control over who can access specific data, providing a vital layer of access control in the system.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106021

F. Key Provision and File Download

The Key Provision and File Download module handles the secure delivery of decryption keys required to access files. Once access is granted, the admin generates a decryption key for the requested file and securely transmits it to the requesting node. The node uses this key to decrypt the file for download. If an incorrect key is entered, the system blocks the download to prevent unauthorized file access. This module is crucial for ensuring that only authorized nodes with the correct keys can retrieve the content. It guarantees that the decryption process is handled securely and prevents any misuse of the files. The Key Provision and File Download module ensures the final stage of secure file retrieval is conducted under strict control and protection.

VI. CONCLUSION

In conclusion, we have introduced a new key management framework for fog computing based on Secure Group Key Management (SGKM). This approach enables end users to securely send encrypted messages to selected fog nodes without the need for a trusted third party. The SGKM scheme 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 proven under the decision BDHE assumption within the standard model, ensuring its reliability. A key advantage of SGKM is its ability to manage dynamic participation while maintaining high security levels. However, the current scheme requires the user to have prior knowledge of the fog node structure. As future work, it would be valuable to explore a key management solution that eliminates the need for such structural knowledge, thereby enhancing scalability and adaptability in diverse and evolving fog computing scenarios.

REFERENCES

1. R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,” Future Generation Comput. Syst., vol. 78, pp. 680–698, 2018.
2. D. Koo, Y. Shin, J. Yun, and J. Hur, “A hybrid deduplication for secure and efficient data outsourcing in fog computing,” in Proc. Int. Conf. Cloud Comput. Technol. Sci., 2016, pp. 285–293.
3. D. Koo and J. Hur, “Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing,” Future Generation Comput. Syst., vol. 78, pp. 739–752, 2018.
4. C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, “CCA-secure ABE with outsourced decryption for fog computing,” Future Generation Comput. Syst., vol. 78, pp. 730–738, 2018.
5. D. Boneh and A. Silverberg, “Applications of multilinear forms to cryptography,” Contemporary Math., vol. 324, no. 1, pp. 71–90, 2002.
6. S. Garg, C. Gentry, and S. Halevi, “Candidate multilinear maps from ideal lattices and applications,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2013, pp. 1–17.
7. Y. Hu and H. Jia, “Cryptanalysis of GGH map,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2016, pp. 537–565.
8. E. Bresson, O. Chevassut, and D. Pointcheval, “Provably authenticated group Diffie Hellman key exchange - The dynamic case,” in Proc. Int. Conf. Theory Appl. Cryptology Inf. Secur., 2001, pp. 290–309.
9. E. Bresson, O. Chevassut, and D. Pointcheval, “Dynamic group Diffie-Hellman key exchange under standard assumptions,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2002, pp. 321–336.
10. H. Kim, S. Lee, and D. Lee, “Constant-round authenticated group key exchange for dynamic groups,” in Proc. Int. Conf. Theory Appl. Cryptology Inf. Secur., 2004, pp. 245–259.
11. R. Dutta and R. Barua, “Provably secure constant round contributory group key agreement in dynamic setting,” IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007–2025, May 2008.
12. M. Naor and B. Pinkas, “Efficient trace and revoke schemes,” in Proc. Int. Conf. Financial Cryptography, 2000, pp. 1–20.
13. D. Phan, D. Pointcheval, and M. Strefler, “Decentralized dynamic broadcast encryption,” in Proc. Int. Conf. Secur. Cryptography Netw., 2012, pp. 166–183.
14. Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, “Asymmetric group key agreement,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2009, pp. 153–170.
15. L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “Identity-based authenticated asymmetric group key agreement protocol,” in Proc. Annu. Int. Comput. Combinatorics Conf., 2010, pp. 510–519.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com