e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711116

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Scalable Cryptographic Solutions for Dynamic Fog Computing Environments

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 extends cloud computing by enabling decentralized data processing at the network edge, improving efficiency and reducing latency. However, the distributed nature of fog nodes introduces security challenges, particularly in establishing secure communication. To address this, we propose two key management schemes for secure communication in fog systems. The first scheme, Dynamic Contributory Key Encryption (DCKKE), allows fog nodes to collaboratively establish a shared encryption key and individual decryption keys without relying on a trusted third party. Users can encrypt messages using a public encryption key, sending them to selected fog nodes, which can decrypt the messages using their respective decryption keys. The second scheme, Dynamic Contributory Broadcast Encryption (DConBE), enables fog nodes to negotiate both a public encryption key and individual decryption keys in one round, without a trusted dealer. It allows users to encrypt messages under the public key and securely deliver them to selected fog nodes for decryption. Both schemes ensure secure communication, collusion resistance, and adaptability to dynamic fog environments, providing a scalable, resilient, and secure solution for fog computing applications, including IoT and smart devices.

KEYWORDS: Fog Computing, Key Management, Secure Communication, Dynamic Contributory Encryption, Decentralized Security.

I. INTRODUCTION

Conventional cloud computing faces challenges in meeting the requirements of modern latency-sensitive applications due to constrained bandwidth and the significant distance between users and centralized servers. The rapid expansion of connected devices demands a new approach to provide efficient, low-latency services. Fog computing emerges as a viable solution.

Fog computing brings computational resources closer to the network edge, reducing latency and improving efficiency. This architecture supports various real-time applications, enhancing Quality of Service (QoS) and user satisfaction. It is particularly beneficial in scenarios such as smart transportation, industrial automation, and IoT-based systems.

Despite its advantages, the distributed nature of fog nodes presents significant security concerns, especially for communication. This work introduces a Dynamic Contributory Broadcast Encryption (DConBE) framework to establish secure and scalable communication in fog systems without relying on a centralized authority, ensuring flexibility and resilience.

II. EXISTING SYSTEM

While the current fog networks focus on efficient data handling and encryption, they are hindered by issues related to node dynamics and communication overhead:

- Large, dynamic fog systems face challenges in communication and computation due to frequent changes in system membership.
- As fog nodes continuously join and leave the network, maintaining security through effective key management becomes essential.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711116

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Contributory Broadcast Encryption (ConBE) allows fog nodes to collectively establish an encryption key while keeping their individual decryption keys private.
- Users can encrypt messages with the public key and securely send them to selected fog nodes in the system.
- If the Private Key Generator (PKG) is compromised, all messages encrypted with that key pair are vulnerable, necessitating regular key updates to ensure system security.

III. PROPOSED SYSTEM

The proposed system addresses these challenges by incorporating Dynamic Contributory Broadcast Encryption (DConBE) for enhanced security and efficient key management in fog computing. Key features include:

- Enabling fog nodes to negotiate a public encryption key and individual decryption keys in one round, without needing a trusted third party.
- Facilitating the dynamic joining and leaving of fog nodes while ensuring continuous security and integrity of the system.
- Implementing cryptographic puzzles to secure deduplication of encrypted data, addressing data privacy concerns in fog environments.
- Introducing innovative key management schemes that ensure reliable communication channels, filling a gap in current fog computing solutions.
- Providing strong security proofs and practical experimentation to demonstrate the system's feasibility and reliability in real-world scenarios.

IV. ARCHITECTURE DIAGRAM

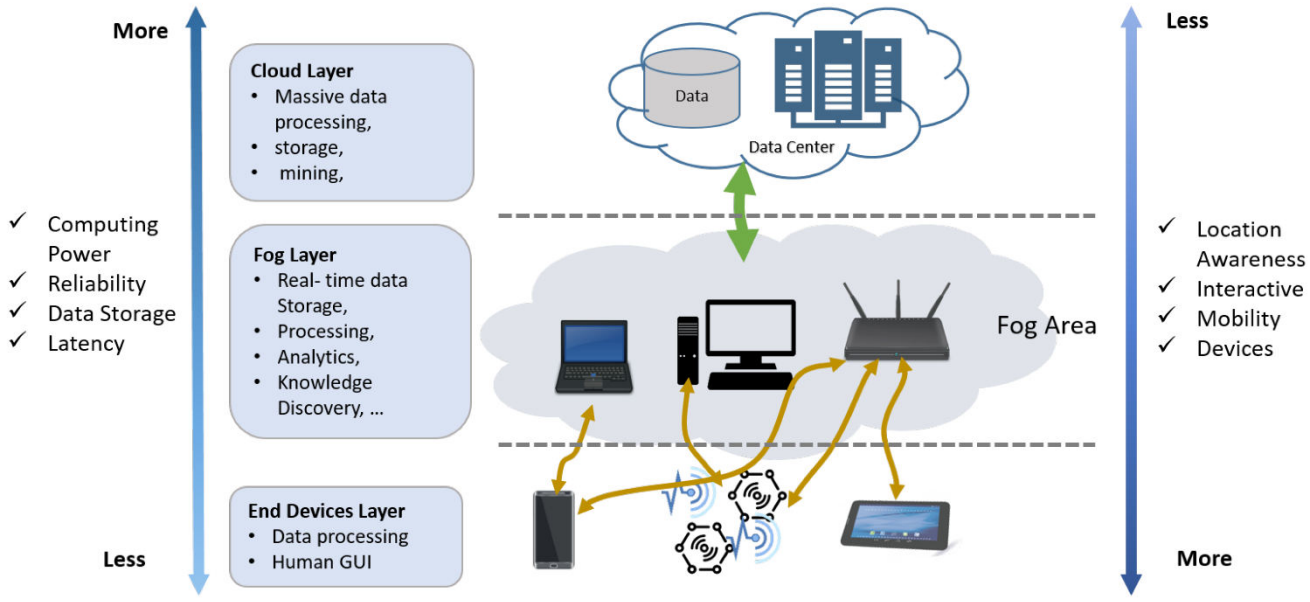

Fig 4.1. Architecture Diagram

A. ARCHITECTURE EXPLANATION

Fog computing is a distributed computing architecture that brings computation and storage closer to the data source, reducing latency and improving efficiency. It consists of three layers: the cloud layer, the fog layer, and the end devices layer. The cloud layer, located at the top of the hierarchy, represents centralized cloud computing resources that handle massive data processing, storage, and mining tasks. It offers high computing power, reliability, and data storage capacity. The fog layer sits between the cloud and end devices, acting as an intermediary layer. It is responsible for real-

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

time data processing, analytics, and knowledge discovery. By providing storage and processing capabilities closer to the data source, the fog layer reduces latency and enables location awareness, interactive mobility, and supports devices with limited processing capabilities. The end devices layer consists of various IoT devices and other edge devices that generate data and may perform some basic data processing and human interface tasks. These devices leverage the fog layer and cloud layer for more complex processing and storage.

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

Fog computing offers several key advantages:

- Reduced Latency: Processing data closer to the source minimizes latency, enabling real-time applications and faster response times.
- Enhanced Scalability: The distributed nature of fog computing allows for easy scaling of resources to accommodate increasing data volumes and device numbers.
- Improved Reliability: By distributing processing and storage across multiple nodes, fog computing can enhance system reliability and fault tolerance.
- Privacy and Security: Processing sensitive data locally at the edge can improve privacy and security by minimizing data transfer to centralized cloud servers.
- Network Offloading: Fog computing can reduce the load on the network by processing data locally, freeing up bandwidth for other critical tasks.

Fog computing is well-suited for a variety of applications, including IoT applications, augmented reality and virtual reality, and autonomous vehicles. However, it also introduces challenges such as complexity and security. Despite these challenges, fog computing is a promising approach for handling the increasing demands of IoT and edge computing. By bringing computation and storage closer to the data source, it offers several advantages in terms of latency, scalability, reliability, privacy, and network efficiency.

V. MODULES

A. Administrator Access Control

The Administrator Access Control module is responsible for safeguarding the entry point into the system by requiring a secure login. Only users with valid credentials (username and password) are allowed to proceed. If the credentials are incorrect, access is denied, and an error message is shown. This process ensures that unauthorized users are unable to enter the system. The administrator also holds the responsibility of managing node tasks, validating permissions, and generating encryption keys. It serves as the security backbone for maintaining controlled access to the system and overseeing the operation of the nodes. By regulating user and admin permissions, the system ensures that unauthorized access is prevented at all levels.

B. Node Interaction Interface

The Node Interaction Interface module enables the smooth operation of nodes after successful authentication. The administrator assigns specific tasks to various nodes, each responsible for performing a designated job and uploading files to the central database. This module facilitates communication between the admin and nodes, allowing for task delegation and status updates. The nodes autonomously execute their tasks but rely on the admin for coordination and file management. It helps build a decentralized environment where nodes work in tandem to fulfill the system's requirements. The Node Interaction Interface ensures that nodes can communicate effectively with the admin and each other while maintaining a secure and coordinated operation.

C. File Encryption and Upload

The File Encryption and Upload module manages the secure transfer of data from nodes to the database. As nodes complete their assigned tasks, they encrypt the files before uploading them, ensuring confidentiality and integrity. The encrypted files are then securely stored in the database, where they are protected from unauthorized access. This module is crucial for maintaining data privacy and protecting sensitive information during transmission.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

After the files are uploaded, they are cataloged with associated metadata, including encryption details, for later retrieval. The system ensures that files remain encrypted in storage, with decryption only permitted through a secure and authorized process. This module safeguards both the upload process and the confidentiality of the data.

D. Access Request Protocol

The Access Request Protocol module handles the process through which one node requests access to a file uploaded by another node. For instance, if Node 2 wants to access a file uploaded by Node 1, it must first send an access request to Node 1. The system ensures that only authorized nodes can send such requests, adding an extra layer of control. File access is not granted automatically, and both the uploading node and the admin must approve the request. This ensures that sensitive data is protected from unauthorized access and only legitimate requests are allowed. The system tracks each request, ensuring transparency and accountability. The Access Request Protocol ensures that all data exchanges follow the proper security protocols.

E. Access Approval Response

The Access Approval Response module is responsible for managing the approval or denial of access requests. When a node requests access to a file, the node that uploaded the file must decide whether to approve or reject the request. If approved, the system sends a response granting the requesting node access to the file. If rejected, a denial message is sent, and the request is discarded. This module ensures that access control remains in place and that files are shared only with authorized nodes. All requests and responses are securely transmitted to prevent unauthorized modifications. The Access Approval Response module ensures that only validated and legitimate requests are processed and acted upon, maintaining data security.

F. Key Distribution and File Retrieval

The Key Distribution and File Retrieval module manages the process of securely distributing decryption keys for file access. After a request is approved, the admin generates a unique decryption key for the requested file and sends it to the node. This key ensures that only the requesting node can decrypt and access the file content. If the node attempts to use an incorrect key, the system prevents the file from being opened. The module plays a key role in the final phase of file access, ensuring that only authorized nodes can retrieve and decrypt files. The system checks the validity of the decryption key before allowing any downloads, preventing unauthorized access. This module ensures the security of files by controlling how and when decryption keys are shared.

VI. CONCLUSION

In conclusion, we have introduced a novel key management approach for fog computing by utilizing Dynamic Contributory Key Encryption (DCKKE) and Dynamic Contributory Broadcast Encryption (DConBE). This approach allows end users to securely transmit encrypted messages to selected fog nodes, without relying on a trusted third party. The DConBE scheme efficiently handles the dynamic nature of fog environments, allowing nodes to seamlessly join or leave the system. The security of our method has been rigorously demonstrated under the decision BDHE assumption within the standard model, ensuring its robustness. One of the key strengths of DConBE is its ability to manage dynamic node participation while maintaining high levels of security. However, it currently requires users to be aware of the fog node structure in advance. As a potential area for future improvement, a key management framework that does not require prior knowledge of node structures could be developed, enabling even greater flexibility and scalability in diverse fog computing scenarios.

REFERENCES

1. J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, “Secure intelligent traffic light control using fog computing,” Future Generation Comput. Syst., vol. 78, pp. 817–824, 2018.
2. M. Burmester and Y. G. Desmedt, “A secure and efficient conference key distribution system,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 1995, pp. 275–286.
3. S. Jiang, “Group key agreement with local connectivity,” IEEE Trans. Depend. Secure Comput., vol. 13, no. 3, pp. 326–339, Jun. 2016.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, and O. Farras, "Bridging broadcast encryption and group key agreement," in Proc. Annu. Int. Conf. Theory Appl. Cryptology Inf. Secur., 2011, pp. 143–160.
5. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and J. A. Manjon, "Contributory broadcast encryption with efficientencryption and short ciphertexts," IEEE Trans. Comput., vol. 65, no. 2, pp. 466–479, Feb. 2016.
6. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf
7. L. Zhang, M. Luo, J. Li, M. Au, K. Choo, T. Chen, and S. Tian, "Blockchain based secure data sharing system for internet of vehicles: A position paper," Veh. Commun., https://doi.org/ 10.1016/j.vehcom.2019.03.003
8. D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in Proc. Annu. Int. Cryptology Conf., 2005, pp. 258–275.
9. D. Boneh and B. Waters, "A fully collusion resistant broadcast, trace, and revoke system," in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 211–220.
10. C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," in Proc. Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59. [21] Y. Dodis and Ilias Siniosoglou, Panagiotis Radoglou-Grammatikis, Georgios Efstathopoulos, Panagiotis Fouliras , and Panagiotis Sarigiannidis " A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments"IEEE transactions on network and service management, vol. 18, no. 2, june 2021
11. Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," in Proc. Secur. Privacy Digit. Rights Manage., 2002, pp. 61–80.
12. J. Kim, W. Susilo, M. Au, and J. Seberry, "Adaptively secure identitybased broadcast encryption with a constant-sized ciphertext," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 679–693, Mar. 2015.
13. F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proc. 1st Edition MCC Workshop Mobile Cloud Comput., 2012, pp. 13–16.
14. S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in Proc. Int. Conf. Wireless Algorithms Syst. Appl., 2015, pp. 685–695.
15. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet Comput., vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com