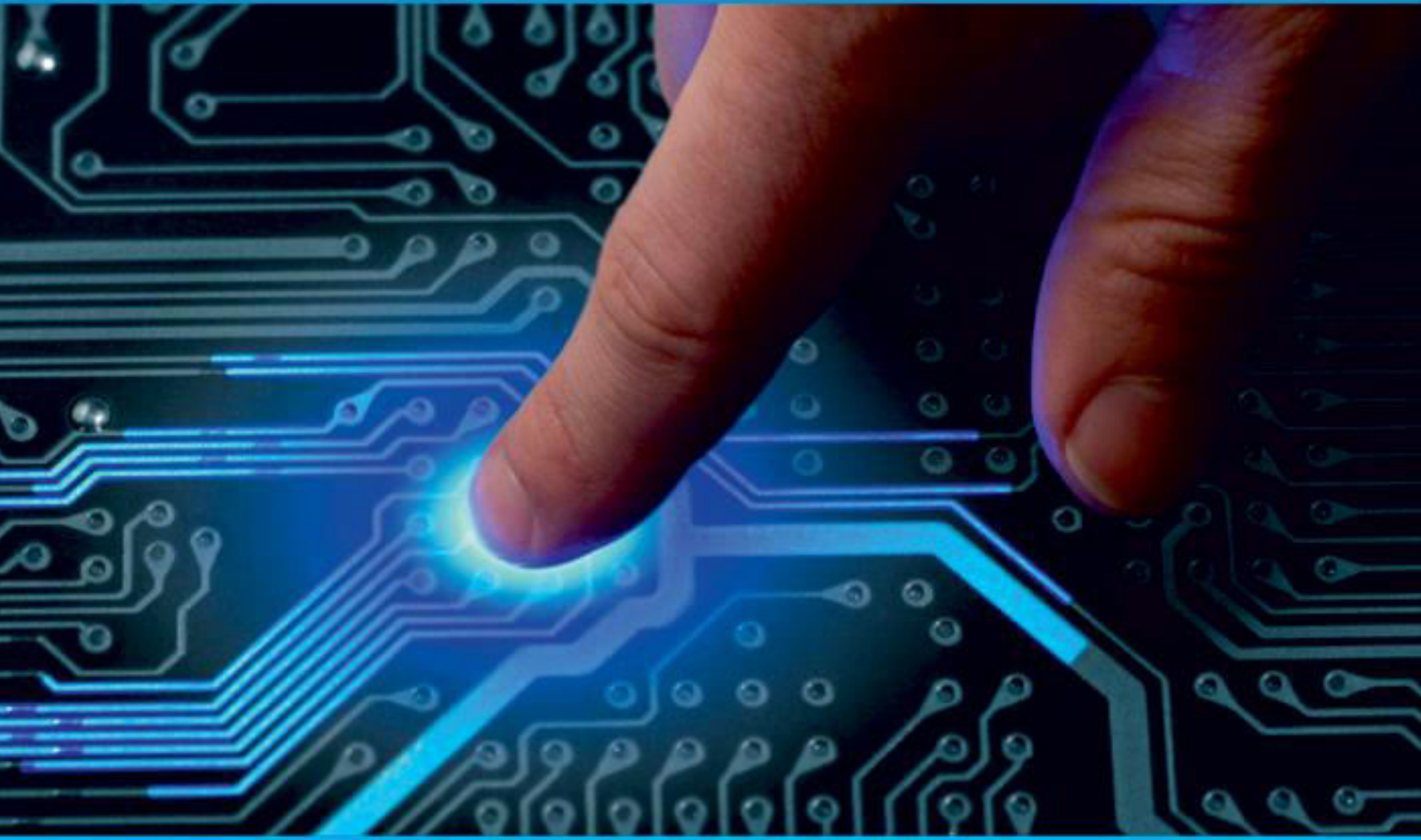
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211120

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Resilient Key Distribution and Encryption Techniques for Fog Node Security

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

Traditional cloud computing struggles to meet the demands of latency-sensitive applications due to limited bandwidth and long distances between servers and users. With the rapid growth of connected devices, a new computing paradigm is required to deliver low-latency and efficient services. Fog computing addresses these limitations effectively.

Fog computing extends cloud capabilities by enabling processing at the network edge, closer to users. This architecture supports real-time applications, enhances Quality of Service (QoS), and caters to diverse scenarios like smart transportation, industrial automation, and IoT systems. It ensures better user experiences in dynamic environment.

However, the decentralized nature of fog nodes introduces security challenges, particularly in communication. This study proposes a Dynamic Contributory Broadcast Encryption (DConBE) scheme to enable secure, scalable communication in fog environments without relying on trusted intermediaries, ensuring robust and adaptable solutions.

II. EXISTING SYSTEM

The present fog computing frameworks prioritize encryption and decentralized processing but encounter difficulties in maintaining continuous security during system changes:

- Communication and computation complexities arise in large, dynamic fog systems due to frequent membership changes.
- Fog nodes dynamically join or leave the system, requiring efficient key management to maintain security.
- Contributory Broadcast Encryption (ConBE) enables fog nodes to negotiate a shared encryption key while retaining individual decryption keys.
- End users can securely send messages to selected subsets of fog nodes using the public encryption key.

- If a Private Key Generator (PKG) is compromised, all communications tied to that key pair are at risk, requiring periodic key updates to mitigate this vulnerability.

III. PROPOSED SYSTEM

The proposed system overcomes these limitations by leveraging Dynamic Contributory Broadcast Encryption (DConBE) for secure key management and reliable communication in fog computing. Key features include:

- The proposed system introduces Dynamic Contributory Broadcast Encryption (DConBE), which enables fog nodes to negotiate a public encryption key and individual decryption keys in a single round without requiring a trusted dealer.
- The DConBE scheme allows fog nodes to dynamically join or leave the fog system, ensuring that security is maintained throughout the system's evolution.
- The system addresses the challenge of secure deduplication of encrypted data in fog environments, utilizing cryptographic puzzles to enhance data security.
- It proposes efficient key management schemes that establish reliable communication channels, a critical aspect that remains unexplored in current fog computing systems.
- The proposed system provides a comprehensive analysis of security and practical implementation, demonstrating the feasibility and effectiveness of the ConBE scheme through experiments and theoretical proofs.

IV. ARCHITECTURE DIAGRAM

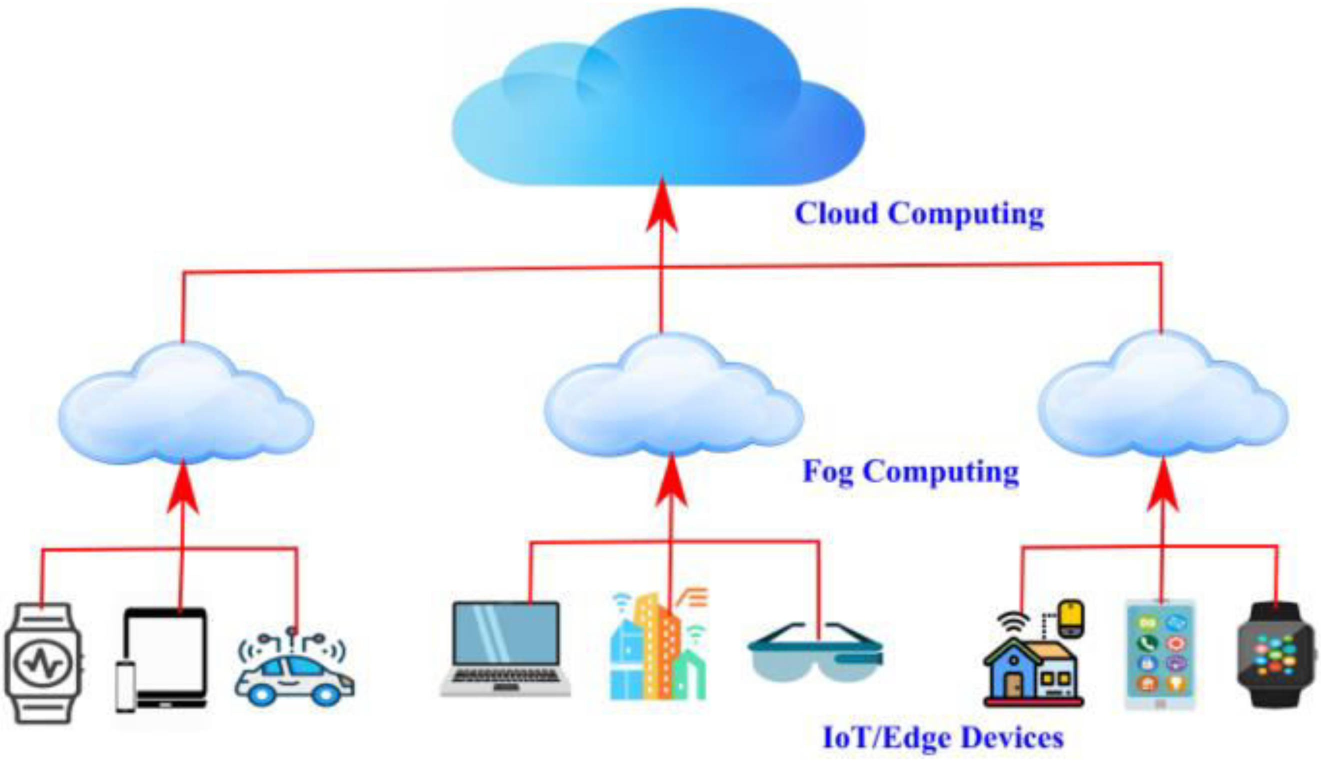


Fig 4.1. Architecture Diagram

A.ARCHITECTURE EXPLANATION

The architecture in the image illustrates a three-tier computing model comprising Cloud Computing, Fog Computing, and IoT/Edge Devices. At the top level, Cloud Computing serves as a centralized platform that provides large-scale data storage, computational power, and extensive analytics capabilities. It acts as the backbone of the entire system. The second level, Fog Computing, is distributed and positioned closer to the edge of the network. This layer ensures that data processing occurs closer to the data source, reducing latency and bandwidth usage, enabling faster decision-making in real-time applications. The third layer consists of IoT/Edge Devices, such as smartwatches, phones, and smart homes, which are directly connected to the fog computing layer. These devices collect data and interact with the fog computing nodes, enabling applications like smart healthcare, transportation, and home automation. Fog nodes act as intermediaries between the IoT devices and the cloud, processing data locally and securely. The architecture ensures seamless interaction between the cloud, fog, and edge layers, enabling efficient and low-latency services for various IoT-based applications.

V. MODULES

5.1. Admin Module

The Admin module is essential for managing access to the system, beginning with a secure login interface. The admin must enter a valid username and password, which are verified against the system's credentials. If the login details are incorrect, access is denied, and an error message is displayed. This process ensures that only authorized individuals can access sensitive areas of the system. The Admin also plays a key role in managing nodes, assigning tasks, and generating decryption keys. This module ensures the system’s security by controlling access and monitoring activities. Additionally, it handles the overall coordination between nodes and users for efficient file management.

5.2. Node Interface

The Node Interface module allows nodes to interact with the system after logging in. After the admin successfully logs in, the system assigns specific tasks to various nodes (e.g., Node 1 to Node 5). Each node is responsible for performing a designated task and uploading the corresponding files into the system's database. This module ensures that the nodes can communicate with the admin and other nodes to confirm task assignments and provide updates. The nodes also send status notifications to the admin, keeping the system well-monitored. The node interface helps in creating a decentralized network, where each node works autonomously while being part of the larger system. It supports the dynamic interaction between different nodes and the admin.

5.3. File Upload

The File Upload module handles the process by which nodes upload data to the central database. As each node completes its assigned task, it encrypts the corresponding file to ensure security before uploading it. The encryption is vital for protecting sensitive information and preventing unauthorized access. Once uploaded, the encrypted files are stored in a centralized database, where they remain secure. The system then registers the file along with its metadata, including the encryption key, to ensure it can be retrieved later. This module is crucial in ensuring data integrity and privacy by safeguarding files during the upload and storage process. The file upload process also includes logging the status of each task, allowing the admin to track progress.

5.4. Request

The Request module allows a node to request access to a file uploaded by another node. If Node 2, for example, wants to access a file uploaded by Node 1, it sends a request to Node 1. The system ensures that these requests are processed securely and that only authorized nodes can send such requests. The requesting node cannot directly access the file in the database unless both the node that uploaded the file and the admin approve the request. This permission-based approach ensures data security and access control across the system. Additionally, each request is logged to maintain transparency and provide a trail of actions for auditing purposes. The Request module acts as a gatekeeper, ensuring that only valid requests from trusted nodes are entertained.

5.5. Response

The Response module is responsible for handling the file access request made by a node. Once a request is received from a requesting node, the node that uploaded the file can either approve or deny the access. If the request is approved, a response is sent back to the requesting node, granting permission to access the file. If the request is rejected, the system sends a denial response, and the requesting node is not permitted to access the file. This module ensures that nodes cannot bypass the access control mechanism and ensures that files are only accessible to authorized parties. The response is sent securely to prevent tampering or unauthorized modification. The system tracks and logs each request and response to ensure accountability.

5.6. Admin (Send Key) and Download

Once a node receives a positive response for file access, the Admin generates and sends a decryption key necessary to open the file. The decryption key is unique to each file and ensures that only the requesting node can decrypt the file. The Admin's role in sending the key adds an additional layer of security by ensuring that the key is only provided to authorized nodes. If the requesting node tries to use an incorrect or expired key, the file will not be accessible. This module controls the final stage of file access by ensuring that only nodes with valid authorization can download and decrypt files. After receiving the key, the node can proceed to download the original file content from the database. The system verifies the key before allowing the download, preventing unauthorized file access.

VI. CONCLUSION

In conclusion, we have proposed a robust key management scheme for fog computing, leveraging Dynamic Contributory Key Encryption (DCKKE) and Dynamic Contributory Broadcast Encryption (DConBE). Our DConBE scheme allows end users to securely send encrypted messages to a selected subset of fog nodes, eliminating the need for a trusted dealer. This scheme efficiently supports dynamic node participation, enabling fog nodes to join or leave the system with minimal overhead. The security of the proposed system is validated under the decision BDHE assumption in the standard model, ensuring its robustness. A notable advantage of DConBE is its ability to handle dynamic fog systems while maintaining confidentiality. However, the scheme currently requires the user to know the structure of fog nodes in advance. Future work could focus on developing a key management solution that does not depend on prior knowledge of the fog node structure, further enhancing its scalability and flexibility in large and highly dynamic fog environments.

REFERENCES

1. P. Mell, and T. Grace, "The NIST Definition of Cloud Computing," NIST Special Publication, 2011, pp. 800–145.
2. J. Li, L. Zhang, K. Liu, H. Qian, and Z. Dong, "Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, 2016.
3. L. Zhang, X. Meng, K.R. Choo, Y. Zhang, and F. Dai, "PrivacyPreserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud", IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2018.2797190.
4. R. Meulen, "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015," http://www.gartner.com/newsroom/id/3165317 (11/10/2015).
5. IDC Market in a Minute: Internet of Things, http://www.idc.com/downloads/idc market in a minute iot infographic.pdf.
6. L. Zhang, and J. Li, "Enabling Robust and Privacy-Preserving Resource Allocation in Fog Computing," IEEE Access, vol. 6, pp. 50384–50393, 2018.
7. M. Chiang, and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.
8. A. Fiat, and M. Naor, "Broadcast Encryption," in Annual International Cryptology Conference (CRYPTO), 1993, pp. 480–491.
9. L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "PrivacyPreserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, 2016.
10. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed Aggregate Privacy Preserving Authentication in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017.
11. X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," Wireless Netw., vol. 25, no. 8, pp. 4737–4750, Nov. 2019.
12. C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, "A secure authenticated and key exchange scheme for fog computing," Enterprise Inf. Syst., vol. 15, no. 9, pp. 1200–1215, Oct. 2021.
13. L. Wang, H. An, and Z. Chang, "Security enhancement on a lightweight authentication scheme with anonymity fog computing architecture," IEEE Access, vol. 8, pp. 97267–97278, 2020.
14. R. Kalaria, A. S. M. Kayes, W. Rahayu, and E. Pardede, "A secure mutual authentication approach to fog computing environment," Comput. Secur., vol. 111, Dec. 2021, Art. no. 102483.
15. Y. Guo, Z. Zhang, and Y. Guo, "Fog-centric authenticated key agreement scheme without trusted parties," IEEE Syst. J., vol. 15, no. 4, pp. 5057–5066, Dec. 2021.
16. M. Hamada, S. A. Salem, and F. M. Salem, "LAMAS: Lightweight anonymous mutual authentication scheme for securing fog computing environments," Ain Shams Eng. J., vol. 13, no. 6, Nov. 2022, Art. no. 101752.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details