A Survey on Privacy Preservation in Fog-Enabled Internet of Things

G Ramesh[1*]. M Madhusudhan Reddy[2] and S M Shamsheer Daula[3]

[1, 3]Associate Professor, Department of ECE, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India -518007
[2]Assistant Professor, Department of ECE, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India – 518007.
ramesh.ece@gprec.ac.in.

Abstract. The Internet of Things (IoT) has revolutionized various aspects of modern life, but it also raises significant privacy concerns. Fog computing, an extension of cloud computing, has developed as a promising solution to mitigate these concerns by processing data closer to the source. This survey provides a comprehensive review of privacy requirements and preservation techniques in fog-enabled IoT. We classify existing solutions into data-oriented, device-oriented, and network-oriented approaches and highlight their strengths and limitations. Our analysis reveals that while important progress has been made, challenges persist, particularly in ensuring scalability, flexibility, and real time processing.

Keywords: IoT, data-oriented, device-oriented, scalability and flexibility.

1 Introduction

The IoT has become ubiquitous, connecting billions of devices worldwide. However, this increased connectivity raises concerns about data confidentiality and security. Fog computing has arose as a solution to address these concerns by processing data closer to the source, reducing expectancy and improving real-time processing as shown in figure 1.

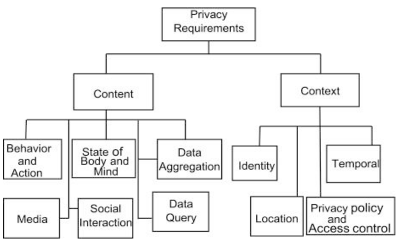

Fig. 1. Privacy Requirements in Fog

B. S. Babu et al. (eds.), *Proceedings of International Conference on Advanced Materials, Manufacturing and Sustainable Development (ICAMMSD-2024)*, Advances in Engineering Research 257,
https://doi.org/10.2991/978-94-6463-662-8_62

Table 1. Comparisons of various privacy techniques

S. No.	Privacy Preservation Technique	Comparative features
1.	Privacy Requirements in IoT	1. Data Privacy 2. Data Reliability 3. Authentication 4. Access Regulation 5. Anonymity
2.	Fog-Enabled IoT Architecture	1. IoT Devices 2. Fog Nodes 3. Cloud Computing
3.	Data-Oriented Approaches	1. Encryption (e.g., AES, RSA) 2. Data Obfuscation 3. Data Anonymization
4.	Device-Oriented Approaches:	1. Secure Boot Mechanisms 2. Secure Firmware Updates 3. Intrusion Detection Systems
5.	Network-Oriented Approaches	1. Secure Communication Protocols (e.g., SSL/TLS) 2. Network Segmentation 3. Access Control Lists

As displayed in the table 1, to resolve these issues, fog computing has been presented for IoT network edges giving low dormancy, calculation, and capacity administrations. In this study, we exhaustively audit and group security prerequisites for a top to bottom comprehension of protection suggestions in IoT applications. In light of the arrangement, we feature continuous exploration endeavors and restrictions of the current protection conservation procedures and guide the current IoT plans with fog empowered IoT plans to expand on the advantages and upgrades that fog empowered IoT can acquire to save information security IoT applications. In conclusion, we identify key examination difficulties and point out future exploration headings.

2 Challenges and Limitations

Scalability

Scalability is a significant challenge in IoT privacy due to the vast number of devices connected to the internet. As the IoT ecosystem grows, handling and securing the data produced by these devices becomes increasingly complex. Key issues include:

- Data storage and processing capacity

- Network bandwidth and congestion
- Ensuring consistent security protocols across diverse devices

Flexibility

IoT devices and systems often lack flexibility, making it difficult to adapt to changing privacy requirements or evolving security threats. Challenges include:
- Inability to update firmware or software on older devices
- Limited configurability of privacy settings
- Incompatibility between different devices and systems

Real Time Processing

Real-time processing is crucial for many IoT applications, such as smart homes, industrial automation & healthcare monitoring. However, ensuring real-time processing while maintaining privacy is challenging due to:
- Latency issues in data transmission and processing
- Ensuring secure data handling at the edge or in the cloud
- Balancing processing speed with data encryption and anonymization

Energy Efficiency

IoT devices frequently have limited power resources, making energy efficiency a critical consideration for privacy measures. Challenges include:
- Power-consuming encryption and decryption processes
- Energy-intensive data transmission and communication protocols
- Limited battery life for devices with continuous data transmission requirements

Standardization

Standardization is essential for ensuring interoperability and effective privacy measures in IoT. However, the lack of standardization in IoT privacy leads to:
- Inconsistent data formats and protocols
- Difficulty in comparing and evaluating different privacy solutions
- Incompatibility between devices and systems from different manufacturers

Additional IoT privacy challenges and limitations include:
- Data protection and ownership
- Lack of transparency and user consent
- Insufficient regulation and governance
- Vulnerabilities in device and system design
- Dependence on third-party services and data analytics

To address these tasks, examiners and developers are exploring innovative solutions, such as:
- Lightweight encryption and security protocols
- Edge computing and fog computing architectures
- Privacy-preserving data processing and analytics
- Standardized privacy frameworks and regulations
- Energy-efficient hardware and software designs

Future research directions for IoT privacy and security:

3 Developing Lightweight Encryption Algorithms

Objective: Design encryption algorithms that minimize computational overhead, energy consumption, and memory usage while maintaining security.

Research Focus
- Symmetric-key algorithms (e.g., AES variants)
-- Hash-based signatures (e.g., SPHINCS)
- Quantum-resistant algorithms (e.g., lattice-based cryptography)
- Homomorphic encryption

Challenges
- Balancing security and performance
- Ensuring side-channel attack resistance
- Adapting to evolving cryptographic standards

4 Improving Secure Firmware Update Mechanisms

Objective: Develop efficient, secure, and scalable firmware update processes to prevent vulnerabilities.

Research Focus
- Secure boot mechanisms
- Rollback attack prevention
- Differential updates (reducing update size)
- Firmware validation and verification
- Automated update testing and validation

Challenges
- Ensuring update authenticity and integrity
- Preventing DoS attacks during updates
- Supporting diverse hardware platforms

5 Designing Scalable and Flexible Fog Architectures

Objective: Create fog computing architectures that efficiently manage IoT data, ensuring security, scalability, and flexibility.

Research Focus

- Distributed data processing and storage
- Edge computing and fog node placement strategies
- Resource allocation and management
- Fog-enabled security and privacy protocols
- Integration with cloud and IoT devices

Challenges

- Managing heterogeneous devices and networks
- Ensuring real time processing and low latency
- Scalability, adaptability

6 Investigating Blockchain-Based Solutions

Objective: Explore blockchain technology for IoT security, privacy, and data management.

Research Focus

- Secure data sharing and ownership
- Decentralized identity management
- Blockchain-based access control
- Smart contract-based security policies
- Scalability and performance optimization

Challenges

- Scalability and energy efficiency
- Integration with existing IoT infrastructure
- Regulatory and standardization issues

Conclusion

This survey highlights the importance of preservation of privacy in fog-enabled IoT and provides a comprehensive overview of existing solutions. While progress has been made, challenges persist, and future research directions are necessary to ensure secure and private IoT applications.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. M. Symeonides, Z. Georgiou, D. Trihinas, G. Pallis and M. D. Dikaiakos, Fogify: A Fog Computing Emulation Framework, *2020 IEEE/ACM Symposium on Edge Computing (SEC)*, San Jose, CA, USA, pp. 42-54, (2020).
2. Abubacker, Nirase & Rana, Muhammad Ehsan & Raheem, Mafas. Fog Computing Applications, (2023).
3. Jeyabose, Andrew & Karthikeyan, J.. Privacy-Preserving Internet of Things: Techniques and Applications. International Journal of Engineering and Advanced Technology. 8. 3229-3234. (2019).
4. Alrawais, Arwa & Alhothaily, Abdulrahman & Hu, Chunqiang, Cheng, Xiuzhen. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing. 21. 34-42, (2017).
5. Li, Tian & Wang, Huaqun & He, Debiao & Yu, Jia. (2022). Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT. IEEE Internet of Things Journal. 9. 1-1. 10.1109/JIOT.2022.3147925. (2022).