International Journal of Computer Techniques–IJCT Volume 13 Issue 1, Jan-Feb - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

An Analytical Study of Security Mechanisms for Data Theft Attacks in Fog Computing

Vina Gautam[1], Ujwal Lanjewar[2]

[1]Research Scholar, [1]Assistant Professor, [2]Principal
[1]Department Of Electronics and Computer Science, Rastrasant Tukadoji Maharaj Nagpur University, Nagpur
[1]Dhote Bandhu Science College, Gondia
[2]Shrimati Binzani Mahila Mahavidyalaya, RTM Nagpur University, Nagpur, India
[1]vinal.vina.gtm@gmail.com, [2]ualanjewar@gmail.com

***Abstract:-* Fog computing extends cloud computing capabilities to the network edge, enabling low-latency and real-time services for data-intensive applications. However, the decentralized, heterogeneous, and resource-constrained nature of fog environments makes them highly vulnerable to data theft attacks. Such attacks threaten data confidentiality, user privacy, and overall system integrity across multiple architectural layers. This paper presents an analytical study of security mechanisms designed to mitigate data theft attacks in fog computing. The study examines the fog computing architecture and security model, analyzes the threat landscape and attack surfaces, and classifies major data theft attacks, including eavesdropping, compromised fog nodes, insider attacks, man-in-the-middle attacks, and side-channel leakage. Furthermore, the paper reviews and categorizes existing mitigation techniques such as cryptographic methods, authentication and access control, intrusion detection systems, trust and reputation management, deception-based approaches, and secure storage mechanisms. A comparative analysis highlights the strengths and limitations of these mechanisms. Finally, open challenges and future research directions are discussed to support the development of secure and resilient fog computing systems.**

***Keywords*- Fog Computing; Data Theft Attacks; Security Mechanisms; Data Confidentiality; Privacy Preservation; Intrusion Detection Systems; Access Control**

I. Introduction

The rapid growth of Internet of Things (IoT) devices and latency-sensitive applications has driven the need for computing models that can process data closer to the data source. Fog computing has emerged as a promising paradigm that extends cloud computing services to the network edge, enabling faster response times, reduced bandwidth usage, and improved quality of service. By introducing an intermediate fog layer between end devices and centralized cloud data centers, fog computing supports real-time applications such as smart cities, healthcare monitoring, industrial automation, and intelligent transportation systems.

Despite its advantages, fog computing introduces significant security challenges. Fog nodes are often deployed in open, geographically distributed, and partially trusted environments, making them attractive targets for attackers. The decentralized architecture, dynamic node mobility, and limited computational resources further increase the risk of data theft attacks. These attacks aim to gain unauthorized access to sensitive data during data generation, transmission, processing, or storage, leading to serious privacy and security concerns.

Traditional cloud-centric security solutions are often inadequate for fog environments due to their reliance on centralized control and high computational overhead. As a result, researchers have proposed a wide range of security mechanisms tailored to different layers of the fog architecture. However, no single solution can effectively address all types of data theft attacks.

This paper provides an analytical study of security mechanisms for mitigating data theft attacks in fog computing. It first presents an overview of the fog computing architecture and security model, followed by an analysis of data theft threats and attack surfaces. The paper then classifies major data theft attacks and reviews existing mitigation techniques. A comparative analysis highlights their effectiveness and limitations, and open research challenges are discussed to guide future work in securing fog computing environments.

II. Architectural Overview and Security Model of Fog Computing

Fog computing is a distributed computing paradigm that extends cloud services toward the network edge to enable low-latency data processing and real-time decision-making for delay-sensitive applications. In contrast to conventional cloud systems that depend exclusively on centralized computing facilities, fog computing establishes an intermediary processing tier situated between end-user devices and cloud infrastructure. This intermediate tier executes computational tasks, data storage, and management functions in proximity to the origin of data. This architectural approach improves geographical awareness, accommodates mobile users, and strengthens the system's ability to scale. Such an architectural design enhances location awareness, supports user mobility, and improves system scalability. As a result, fog computing is particularly well suited for Internet of Things (IoT) environments and cyber–physical systems requiring rapid response and efficient resource utilization.

A. Fog Computing Architecture

A typical fog computing architecture is divided into three layers which includes device layer, fog layer, and cloud layer, as shown in Fig. 1.

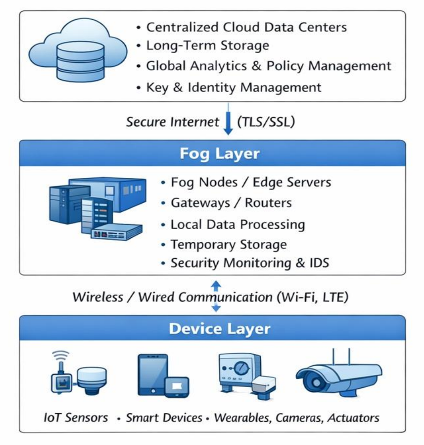
• Centralized Cloud Data Centers
• Long-Term Storage
• Global Analytics & Policy Management
• Key & Identity Management
Secure Internet
(TLS/SSL)
Fog Layer
• Fog Nodes / Edge Servers
• Gateways / Routers
• Local Data Processing
• Temporary Storage
• Security Monitoring & IDS
Wireless / Wired Communication (Wi-Fi, LTE)
Device Layer
IoT Sensors • Smart Devices • Wearables, Cameras, Actuators

Figure 1. Fog Computing Architecture

The device layer contains end-user devices and IoT components such as sensors, actuators, smart cameras, and IoT devices. The device layer is responsible for producing data and performing initial acquisition tasks. However, constrained processing power and limited energy availability necessitate lightweight security solutions, rendering this layer more susceptible to data theft through physical tampering or illicit access. [1], [2].

The fog layer acts as an middleware between the device and cloud layers and includes fog nodes, edge servers, gateways, and routers deployed close to data sources. This layer performs latency-sensitive tasks such as local data processing, filtering, aggregation, and temporary storage. Fog nodes are often geographically distributed and may be operated by third-party service providers, which introduces trust and security challenges. As a result, the fog layer is considered the primary attack surface for data theft attacks in fog computing environments [3], [4].

The cloud layer includes central data centers that handle large-scale data processing, long-term data storage, and overall system control. These data centers usually use strong security measures, but the risk of data theft still exists because of configuration mistakes, unsafe APIs, or stolen login details. The cloud layer also helps manage encryption keys, control user access, and coordinate security rules for the lower layers of the system. [5].

B. Security Model for Fog Computing

Fog computing is spread out and uses different types of devices, so it needs a layered security approach where each layer has its own security role, as shown in Fig. 2. Unlike traditional cloud security that depends mainly on a central system, fog computing uses local security at nearby devices along with overall coordination from the cloud.

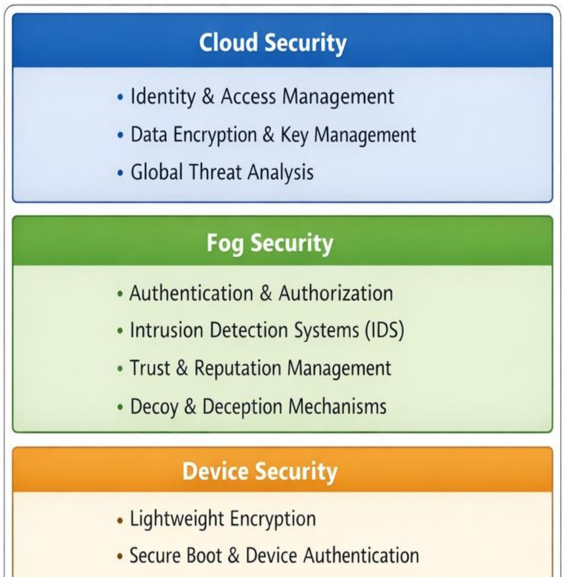
Cloud Security
• Identity & Access Management
• Data Encryption & Key Management
• Global Threat Analysis
Fog Security
• Authentication & Authorization
• Intrusion Detection Systems (IDS)
• Trust & Reputation Management
• Decoy & Deception Mechanisms
Device Security
• Lightweight Encryption
• Secure Boot & Device Authentication

Figure 2. Fog Computing Security Model

The fog security layer is responsible for regulating data access, identifying malicious behavior, and safeguarding sensitive information during both processing and storage. To achieve this, it relies on mechanisms such as user authentication, access authorization, intrusion detection, trust evaluation, and the use of decoy-based protection strategies. [6].

The fog security layer controls who can access data, detect harmful activities, and protect sensitive data while it is being processed and stored. It applies user authentication, access control policies, attack detection mechanisms, trust-based monitoring, and decoy methods to enhance security. These security measures help identify data theft attempts early and reduce the risk of insider attacks within fog nodes. [7], [8].

At the cloud security level, centralized systems are used to manage user identities and control access to data across the entire network. It also manages encryption keys so that communication between devices and fog nodes remains secure. In addition, security logs and alerts collected from multiple fog nodes are sent to the cloud, where advanced analysis is performed. This helps in detecting large-scale or coordinated data theft attacks that may not be visible at individual fog nodes and supports timely security response across the system. [9].

C. Data Theft–Related Security Challenges

Even though fog computing uses a layered security model, it is still vulnerable to data theft attacks because of several basic challenges. Fog nodes are often placed in open or less secure locations, which makes them easy targets for physical attacks. Managing trust is difficult since security decisions are made across many nodes instead of through one centralized authority. In addition, fog nodes may frequently move or join and leave the network, making security monitoring more complex. Limited computing power and storage further restrict the use of strong security techniques. These challenges show the need for specialized security solutions that can protect data without affecting system performance or scalability.

III. Data Theft Attacks in Fog Computing

Fog computing is spread across many locations and does not rely on a single central system, which creates special security problems. Fog nodes are often placed in open and different geographical areas and are not always fully trusted. Because of this, they can be attacked by both outside attackers and insiders. Data theft attacks try to access sensitive information without permission while data is being created, sent, processed, or stored. Such attacks can harm data privacy, user trust, and the overall security of the system.

A. Threat Model and Adversary Capabilities

In fog computing systems, attackers can have different levels of power depending on how much access they have. External attackers usually try to steal data by taking advantage of weak communication links, poor login methods, or software flaws. Internal attackers are more dangerous because they already have permission to access the system. These may include hacked fog nodes or dishonest service providers. Since fog computing does not rely on a single central control system, it is harder to monitor all activities. As a result, insider attacks are especially difficult to detect and prevent in fog computing environments. [10], [11].

In the threat model, it is assumed that attackers can attack any part of the fog computing system. This includes end devices that generate data, fog nodes that process and store data, and cloud services that manage and analyze information. Attackers may focus on just one layer or try to attack multiple layers at the same time. In some cases, attackers from different layers may work together, making the attack more organized and harder to detect. Such coordinated data theft attacks are difficult to stop using traditional security methods, which are usually designed for centralized systems. [12].

B. Attack Surfaces in Fog Computing

Data theft attacks in fog computing can happen at different parts of the system, which are called attack surfaces.

- **Device Layer:** End devices such as IoT sensors and smart devices can be physically accessed or tampered with by attackers. If these devices use insecure software or weak login methods, attackers can directly steal sensitive data from them.
- **Fog Layer:** Fog nodes process and temporarily store data close to users. If a fog node is compromised, attackers can leak data, change it, or secretly forward it to unauthorized locations.
- **Communication Channels:** Data is transferred between devices, fog nodes, and the cloud. If communication is not properly secured, attackers can intercept messages, listen to data exchanges, or replay captured data to gain unauthorized access.
- **Cloud Interfaces:** Cloud services collect large amounts of data from fog nodes. Weak or poorly configured interfaces, unsafe APIs, or stolen login credentials can allow attackers to access stored data without permission.

Together, these multiple attack surfaces make it more difficult to detect and prevent data theft attacks in fog computing environments [13].

C. Classification of Data Theft Attacks

Based on existing literature, data theft attacks in fog computing can be classified into the following categories.

i. Eavesdropping and Traffic Analysis Attacks

In eavesdropping and traffic analysis attacks, attackers secretly listen to data being transmitted between end devices, fog nodes, and cloud servers. Their goal is to capture sensitive information such as user data or system details. Even when the data itself is encrypted, attackers can study communication patterns like data size, timing, and frequency. This analysis can reveal important information about user behavior or system activities, which may lead to privacy breaches in fog computing environments. [14].

ii. Compromised Fog Node Attacks

Fog nodes can be taken over by attackers through malware, software weaknesses, or physical tampering. Once a fog node is compromised, attackers can access sensitive data while it is being processed or stored. They may also change or secretly forward this data without permission. Because fog nodes handle large amounts of local data, such attacks are considered one of the most serious forms of data theft in fog computing environments. [15].

iii. Insider Attacks

Insider attacks are carried out by people or systems that already have authorized access to the fog computing environment, such as fog service providers or system administrators. These insiders may act maliciously or become compromised by attackers. Because they have legitimate access rights, their actions are hard to notice. As a result, insider attacks can lead to the theft of large amounts of sensitive data. [16].

iv. Man-in-the-Middle Attacks

In Man-in-the-Middle attacks, an attacker secretly places themselves between two communicating parties and intercepts or changes the data without being noticed. In fog computing environments, these attacks often happen because of insecure wireless connections or weak authentication methods. This allows attackers to steal sensitive information or manipulate data during transmission [17][18].

v. Data Leakage Through Side Channels

Side-channel attacks take advantage of indirect information leaks, such as differences in processing time, power usage, or memory access behavior. Instead of attacking the data directly, attackers study these patterns to infer sensitive information. Fog nodes are especially vulnerable to such attacks because they often share resources and use virtualization, which can unintentionally expose these side-channel details. [19].

IV. Mitigating Data Theft Attacks

To address data theft risks in fog computing, researchers have proposed multiple security mechanisms that operate at different architectural layers of the system. These security mechanisms are designed to protect sensitive data, control secure access, detect harmful activities, and limit the damage caused by compromised fog nodes. This section examines and categorizes the existing security mechanisms used to defend fog computing environments against data theft attacks.

A. Cryptographic Techniques

Cryptographic techniques play an important role in protecting sensitive data in fog computing systems. Encryption is commonly used to keep data safe while it is being transmitted or stored, so that only authorized users can read it. Because devices and fog nodes have limited computing power, lightweight encryption methods are usually preferred at these layers. Different encryption approaches, such as symmetric encryption, public key encryption, and attribute-based encryption (ABE), are used to control who can access the data and to provide better security at different levels of the fog computing architecture. [20], [21].

Advanced techniques such as homomorphic encryption and secure multi-party computation allow fog nodes to process data without decrypting it. This helps keep the data highly secure. However, these methods require a lot of computing power and processing time. Because of this high overhead, they are difficult to use in real-time fog computing applications where fast response is required. [22].

B. Authentication and Access Control Mechanisms

Authentication and access control mechanisms are important for stopping unauthorized users from accessing sensitive data. These methods help verify the identity of users and devices before allowing them to communicate or use system resources. Different approaches, such as identity-based authentication, certificate-based systems, and lightweight mutual authentication protocols, have been developed to secure communication between end devices, fog nodes, and cloud servers. [23].

Access control models such as role-based access control, attribute-based access control, and capability-based access control are used to decide who is allowed to access data in fog computing systems. These models offer flexible and scalable ways to manage permissions. However, in fog environments, devices and nodes may frequently move or change, and trust is managed in a decentralized way. Because of this, it becomes difficult to apply access control rules consistently across the entire system. [24].

C. Intrusion Detection Systems

Intrusion detection systems (IDS) are commonly used in fog computing to identify data theft attempts and other harmful activities. These systems monitor network traffic, system logs, and user behavior in real time to detect attacks at an early stage. Different IDS methods are used, including signature-based approaches that detect known attacks and anomaly-based approaches that identify unusual behavior. Recent research has also used machine learning techniques to improve detection accuracy and adapt to new attack patterns. [25], [26].

Although intrusion detection systems improve security monitoring, their performance is limited by the low computing power of fog nodes and the lack of sufficient labeled data for training. To address this issue, distributed IDS architectures are often used, where detection tasks are shared across multiple nodes. This helps balance detection accuracy while reducing the processing load on individual fog nodes. [27].

D. Trust and Reputation Management

Trust and reputation management mechanisms are used to evaluate how reliable fog nodes, devices, and service providers are based on their past behavior and interactions. Each entity is given a trust score that reflects how trustworthy it is. These scores help the system identify nodes that may be compromised or acting maliciously, which can reduce the risk of data theft attacks. [28].

Trust-based methods are especially useful for reducing insider attacks, which are hard to detect using traditional security techniques. However, trust models must be designed carefully so that attackers cannot manipulate trust scores by giving false recommendations or working together to mislead the system. [29].

E. Decoy and Deception-Based Security Mechanisms

Decoy and deception-based security methods have recently become promising ways to detect data theft attacks in fog computing systems. These methods use fake data, honeypots, or dummy fog nodes to confuse attackers and observe their actions. When attackers try to access or interact with these decoy resources, security alerts are generated. This helps in detecting data theft attempts early and allows the system to respond quickly. [30].

Decoy-based security methods work especially well against insider attacks and advanced long-term attacks, because genuine users usually have no reason to access fake data. When such data is accessed, it often indicates malicious activity. However, creating decoy systems that look real while using very little computing resources is difficult, especially in dynamic fog computing environments. This remains an open challenge for researchers. [31].

F. Secure Data Storage and Isolation Mechanisms

Secure storage methods are used to protect data while it is being processed or stored at fog nodes. These include secure enclaves, trusted execution environments (TEE), and isolation techniques based on virtualization. Such methods help keep sensitive data separated from untrusted software. Hardware-based security solutions, such as Intel SGX, offer strong protection by isolating data at the hardware level. However, they can also increase system complexity and reduce performance, which limits their practical use in fog computing environments [32].

V. Comparative Analysis of Security Mechanisms

This section compares different security mechanisms that are used to reduce data theft attacks in fog computing systems. The comparison examines how effective each approach is, along with its advantages and limitations, based on the mechanisms discussed in Section 4. Because fog computing is decentralized and involves many different types of devices, no single security solution can protect against all data theft attacks. Therefore, a layered and combined security approach is usually needed to provide better protection.

Cryptographic techniques protect sensitive data by encrypting it while it is being sent or stored. Methods such as attribute-based encryption and secure key management help control who can access the data in a detailed manner. However, these techniques require high processing power, which can be difficult for fog nodes and IoT devices with limited resources [33], [34]. More advanced methods like homomorphic encryption provide better privacy but are usually not suitable for real-time fog applications because they cause high delay and require heavy computation [35].

Authentication and access control mechanisms effectively prevent unauthorized access to fog resources. Lightweight authentication protocols are well-suited for edge environments, but dynamic node mobility and decentralized trust management complicate policy enforcement across multiple fog domains [36]. Furthermore, access control mechanisms alone are insufficient to address insider threats, where attackers already possess legitimate credentials.

Intrusion detection systems (IDS) play a critical role in identifying anomalous behavior and data exfiltration attempts. Machine learning–based intrusion detection systems have shown good accuracy in detecting attacks. However, they usually need large amounts of training data and can generate false alarms in highly dynamic fog computing environments [37], [38]. Distributed intrusion detection systems reduce the workload on individual nodes, but they make coordination between nodes more complex.

Trust and reputation mechanisms help identify compromised or malicious fog nodes, especially in reducing insider attacks. These methods continuously assess node behavior and assign trust values, but they can be affected by collusion and false feedback if not properly designed [39].

Decoy and deception-based methods protect systems by tricking attackers and detecting unauthorized access attempts. These methods work well against insider attacks and long-term threats because normal users usually do not interact with fake data or resources. However, creating decoy data that looks real while keeping system overhead low is still a challenging problem [40], [41].

Overall, the comparison shows that no single security method is enough to protect fog computing systems from data theft attacks. Instead, combining multiple security techniques—such as encryption to protect data, access control to limit unauthorized use, intrusion detection to identify attacks, trust management to detect malicious nodes, and deception techniques to trap attackers—provides much stronger protection. These hybrid security models improve the system's ability to detect attacks early, limit damage, and adapt to different threat scenarios in fog computing environments.

Table 1. Security Mechanisms vs. Data Theft Attacks in Fog Computing

Security Mechanism	Eavesdropping	MitM Attacks	Compromised Fog Nodes	Insider Attacks	Side-Channel Attacks	Key Limitations
Cryptographic Techniques	✓	✓	✕	✕	✕	High computation overhead
Authentication & Access Control	✕	✓	✕	✕	✕	Ineffective against insiders
Intrusion Detection Systems	✓	✓	✓	✓	✕	False positives, training cost
Trust & Reputation Management	✕	✕	✓	✓	✕	Vulnerable to collusion
Decoy & Deception-Based Mechanisms	✕	✕	✓	✓	✕	Deployment and maintenance overhead
Secure Enclaves / Isolation	✕	✕	✓	✕	✓	Hardware dependency

✓ = Effective ✕ = Limited / Not effective

VI. Open Challenges and Future Research Directions

Despite significant progress in developing security mechanisms for mitigating data theft attacks in fog computing, several open challenges remain. One major challenge is the resource limitation of fog nodes and edge devices, which restricts the use of strong cryptographic techniques and continuous security monitoring. Future research should focus on designing lightweight yet effective security solutions that balance protection with performance.

Another challenge is dynamic node mobility and scalability. Fog environments frequently change as devices join, leave, or move across networks, making consistent security policy enforcement difficult. Adaptive and context-aware security mechanisms that can adjust to changing network conditions are needed.

Insider threats and trust management also remain difficult to address due to decentralized control and limited global visibility. Future work should explore robust trust and reputation models that are resilient to false feedback and collusion attacks.

Additionally, machine learning–based intrusion detection systems face challenges related to data availability, false positives, and model adaptability. Research is required to develop lightweight, explainable, and privacy-preserving learning models suitable for fog environments.

Finally, while decoy and deception-based techniques show promise, maintaining realistic decoy systems with minimal overhead remains challenging. Future research should investigate automated and scalable deception strategies. Addressing these challenges will be critical for building secure, scalable, and privacy-preserving fog computing systems.

VII. Conclusion

Fog computing improves low-latency data processing but introduces serious risks of data theft due to its decentralized nature. This paper analyzed key data theft attacks and existing security mechanisms in fog computing. The study highlights that no single technique is sufficient and that layered, hybrid security approaches offer better protection. Future work should focus on lightweight and adaptive security solutions for dynamic fog environments.

References

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," Proc. ACM MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 2012, pp. 13–16.

[2] 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, Dec. 2016.

[3] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," *Proc. IEEE HotWeb*, Washington, DC, USA, 2015, pp. 73–78.

[4] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, Jan. 2018.

[5] P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, and A. Y. Zomaya, "Survey on fog computing: Architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, Nov. 2017.

[6] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, Mar.–Apr. 2017.

[7] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1826–1857, 2018.

[8] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A framework for privacy-preserving authentication of IoT devices in fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3656–3668, Apr. 2019.

[9] N. Santos, K. P. Gummadi, and R. Rodrigues, "Toward trusted cloud computing," *Proc. USENIX HotCloud*, San Diego, CA, USA, 2009.

[10] Y. Xiao and M. Krunz, "Distributed detection of insider attacks in fog computing," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 748–761, Mar. 2017.

[11] Z. Guan, X. Liu, and L. Wu, "Trust management for fog computing," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 88–94, Jan. 2018.

[12] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, Feb. 2018.

[13] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[14] C. Song, J. Zhang, and W. Xu, "Traffic analysis attacks in IoT networks," *IEEE INFOCOM Workshops*, Honolulu, HI, USA, 2018.

[15] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and privacy in smart city applications," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[16] J. Liu, Y. Xiao, and C. Chen, "Insider attack detection in fog computing," *Future Generation Computer Systems*, vol. 82, pp. 1–12, May 2018.

[17] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015.

[18] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Cyber-physical-social systems: A state-of-the-art survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 389–425, 2020.

[19] Y. Yarom and K. Falkner, "FLUSH+RELOAD: A high resolution, low noise, L3 cache side-channel attack," *USENIX Security Symposium*, San Diego, CA, USA, 2014.

[20] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2007.

[21] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Secure data sharing in fog computing using attribute-based encryption," *IEEE Access*, vol. 6, pp. 37544–37553, 2018.

[22] C. Gentry, "Fully homomorphic encryption using ideal lattices," *Proc. ACM STOC*, Bethesda, MD, USA, 2009.

[23] L. Zhou, Y. Li, K. Chen, and Y. Nan, "Lightweight authentication protocol for fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2793–2804, Apr. 2019.

[24] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Access control in the Internet of Things," *Computer Networks*, vol. 112, pp. 237–262, Jan. 2017.

[25] Y. Meidan et al., "N-BaIoT: Network-based detection of IoT botnet attacks," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, Jul.–Sep. 2018.

[26] A. A. Diro and N. Chilamkurti, "Distributed attack detection using deep learning approach," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 56–62, Feb. 2018.

[27] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning-based intrusion detection system for fog computing," *IEEE Access*, vol. 7, pp. 164034–164047, 2019.

[28] Z. Yan, P. Zhang, and A. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, Jul. 2014.

[29] S. Wang, J. Zhang, and Y. Zhang, "Trust evaluation in fog computing," *IEEE Access*, vol. 7, pp. 43690–43702, 2019.

[30] N. K. Sharma and S. K. Sood, "Decoy-based data protection for fog computing," *Computers & Security*, vol. 88, Jan. 2020.

[31] S. Stolfo et al., "Decoy documents: Detecting insider threats," *Proc. ACM CCS Workshop*, Raleigh, NC, USA, 2012.

[32] V. Costan and S. Devadas, "Intel SGX explained," *IACR Cryptology ePrint Archive*, 2016.

[33] H. Almutairi, M. Aldossary, and A. Alqahtani, "Security challenges and solutions in fog computing," *IEEE Access*, vol. 7, pp. 13673–13686, 2019.

[34] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things," *Future Generation Computer Systems*, vol. 56, pp. 684–700, Mar. 2016.

[35] M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, "Disease prediction by machine learning over big data from healthcare communities," *IEEE Access*, vol. 5, pp. 8869–8879, 2017.

[36] S. Yi, C. Li, and Q. Li, "A survey of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 37–42, 2015.

[37] K. Salah, M. H. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[38] L. Nguyen et al., "Federated learning for intrusion detection," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1626–1642, 2021.

[39] T. Nguyen, D. Hoang, and P. Niyato, "A survey of trust management in distributed systems," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[40] S. Chakraborty et al., "Adversarial attacks and defenses," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 72–78, 2019.

[41] M. Fraunholz et al., "HoneyFog: Decoy-based security for fog computing," *IFIP Networking Conference*, 2018.

[42] J. Salem et al., "Behavior-based insider threat detection," *Computers & Security*, vol. 87, 2019.

[43] X. Li, J. Liu, and S. Kumari, "Dynamic trust management for fog computing," *Future Generation Computer Systems*, vol. 92, pp. 749–760, 2019.

[44] Q. Yang et al., "Federated learning," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, 2019.

[45] B. Biggio and F. Roli, "Wild patterns: Ten years after adversarial machine learning," *Pattern Recognition*, vol. 84, pp. 317–331, 2018.