International Journal of Management Science Research, Vol.9, Issue 2, (Feb) 2026
ISSN 2536-605X
DOI: 10.53469/ijomsr.2026.09(02).10

Research on Security Protection Technologies for Edge Computing

Bai Fan, Ye Tao

School of Intelligence Science and Engineering, Qinghai Minzu University, Xining 810007, China

Abstract: ***Edge computing deploys computing resources at the network edge to provide users with services featuring low latency and low energy consumption. Nevertheless, security threats including node deception, data breaches and cyber-attacks make it impossible to achieve secure computation offloading. This paper expounds the relevant theories and technologies of edge computing, investigates the security threats during computation offloading, summarizes the existing protection techniques, and explores the challenges and potential research trends.***

Keywords: Edge Computing; Identity Authentication; Access Control; Intrusion Detection; Privacy Protection.

1. INTRODUCTION

To alleviate the problems of high cost and significant latency in traditional cloud computing, PG Lopez et al. [1] proposed edge-centric computing, namely Edge Computing (EC), in 2015. Its core idea is to “provide users with reliable and stable services nearby” [2]. Various tasks generated by devices are offloaded to nearby edge servers, which provide computing and storage resources to process these offloaded tasks. This can effectively alleviate the pressure on the cloud and improve service quality.

However, edge computing faces several security challenges due to the large number of heterogeneous terminal devices with varying security levels [3]. Tasks offloaded to edge servers face a more complex and dynamic environment. Nodes in edge networks are widely deployed with weak single-point defense capabilities, making them vulnerable to attacks. Additionally, numerous unauthorized or unauthenticated nodes may attempt unauthorized access or tampering, thereby damaging the network' s integrity and stability. Roman and Yi et al. [4], [5] assumed that all participants are untrustworthy and demonstrated the vulnerabilities and threats in EC.

Most existing academic studies on edge computing discuss single security techniques and a comprehensive investigation of secure offloading mechanisms is still insufficient. This particular study conducts a comprehensive summary of the security threats that emerge during each stage of task offloading and offers a systematic review of the relevant security protection technologies.

2. OVERVIEW OF EDGE COMPUTING

2.1 System Architecture

Edge computing represents a distributed architecture that consists of three key components: mobile devices, edge servers, and the cloud, as shown in Figure 1. These mobile devices, which can be smartphones or Internet of Things devices, connect to the Internet through base stations and subsequently gain access to the cloud.

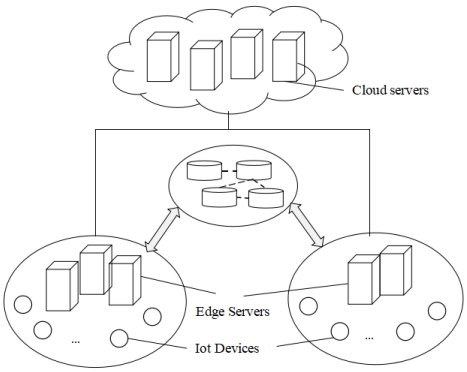

Figure 1: A Multi-user and Multi-edge Server Computing Architecture

2.2 Computation Offloading

With the increasing real-time demands of applications like intelligent transportation and online gaming, computation offloading has emerged as an increasingly pivotal technology. Computation offloading decisions are made based on task properties, network conditions, edge server resource availability, and other related factors. These decisions mainly involve whether to offload computing tasks, the proportion of tasks to be offloaded, and the selection of target offloading servers.

Offloading strategies can be divided into partial offloading and full offloading, which should be flexibly configured according to the actual needs of different application scenarios. The overall offloading process is shown in Figure 2. After confirming the offloading demand, we first evaluate whether the target server is capable of executing the task. If capable, corresponding computing resources are allocated accordingly. Finally, we verify whether offloading can meet the predefined optimization objectives. If satisfied, the task is offloaded to the edge server; otherwise, it is executed locally.

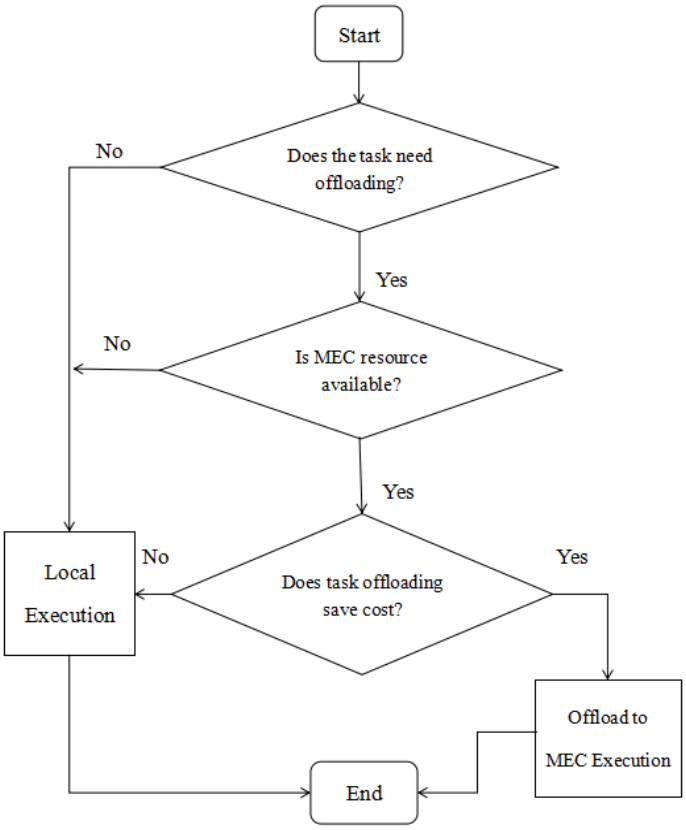

Figure 2: Process of Computation Offloading

2.3 Typical Applications

In logistics delivery, edge computing can cooperate with terminal devices such as drones and robots to perform delivery tasks. It can obtain real-time traffic information, dynamically adjust delivery routes, and avoid obstacles, thereby effectively improving delivery efficiency [6].

In the agricultural field, edge computing can collaborate with drones, soil sensors, plant protection equipment, and other devices to achieve crop growth monitoring, pest and disease identification, and variable-rate plant protection, thereby reducing pesticide usage and improving agricultural production efficiency.

In the context of smart cities, edge computing integrates data collected from drones, intersection monitors, vehicle terminals and other devices. By performing real-time data analysis, it can identify traffic congestion and accident scenes, thus supporting dynamic traffic signal control, road condition evaluation and travel route recommendation.

In power inspection scenarios, edge computing integrated with drones, intelligent inspection robots, portable sensing devices, and other equipment enables rapid coverage of complex areas such as remote and high-altitude locations, and supports real-time processing of inspection images and sensing data. Studies show that using drones equipped with edge computing devices for power inspection, combined with an improved YOLOv5 model and a self-calibrated convolution algorithm, improves inspection efficiency by approximately three times [7].

3. SECURITY THREAT ANALYSIS

During the offloading process of edge computing, key scenarios including device access, offloading decision-making, communication transmission and edge processing are exposed to diverse security threats. These threats mainly fall into five categories: access security, data security, communication security, node security and offloading security, which correspond to the risks present in the four aforementioned scenarios.

Based on their inherent characteristics, these threats can be further divided into common security threats and special security threats. The latter are caused by the unique properties of computation offloading. Specifically, the first four categories belong to common security threats, while special security threats primarily focus on location privacy threats and usage pattern privacy threats, both induced by the distinct characteristics of offloading.

3.1 Common Security Threats

As the primary barrier to network security, device access control prevents unauthorized system penetration. The infiltration of numerous counterfeit terminal devices that attempt to implement illicit modifications or launch distributed denial-of-service (DDoS) attacks poses a direct threat to network integrity and operational stability.

Transmission channels introduce two distinct categories of security risks. On one hand, passive and active attacks such as eavesdropping, tampering and man-in-the-middle interception can compromise data confidentiality and integrity, ultimately leading to irrational offloading decisions. On the other hand, replay and DDoS attacks achieve malicious goals by exhausting the computational and bandwidth resources of terminals, infrastructure, and edge servers. Replay attacks can be effectively curbed through the use of random nonces and timestamp validation. In contrast, mitigating DDoS attacks demands a multitiered defense strategy. Specifically, the physical layer employs sensing techniques to pinpoint attack sources, the network layer carries out real-time traffic analysis, and the application layer implements reliable offloading mechanisms to guarantee service availability.

Link instability also reduces communication quality by increasing the bit error rate. Furthermore, signal occlusion causes attenuation, which may weaken or even cut off the connection between end devices, network infrastructure, and edge servers. Such interruption of communication continuity frequently results in the failure of critical task offloading. In addition, communication links of infrastructure are vulnerable to sophisticated attacks such as signal hijacking and spoofing attacks. Finally, offloading private data to edge nodes forms a new attack surface beyond the user' s security perimeter.

The large scale and geographically distributed deployment of network infrastructure make real-time monitoring difficult, leading to potential service outages caused by human sabotage or environmental factors. Most critically, a malicious edge server disguised as a legitimate node can abuse its processing authority to steal sensitive user data for illegal transactions or tamper with task data during execution.

3.2 Special Security Threats

For network infrastructure, irrational offloading strategies triggered by internal malicious nodes may result in resource occupation and exhaustion. Meanwhile, external attackers are capable of intercepting and tampering with task data or decision commands via vulnerable wireless channels. In the event that the edge server accepts counterfeit information unknowingly and executes subsequent procedures, it may give rise to task interruptions or even substantial economic losses. In addition, malicious edge servers are able to estimate the distance to users according to their offloading state. More importantly, coordinated information sharing among multiple malicious servers enables them to achieve precise user localization, which introduces severe location privacy disclosure risks. Regarding the threat of usage pattern leakage, long-term monitoring of offloading data by edge servers can be realized when users persistently choose a fixed edge server for task offloading, allowing the server to deduce users' behavior habits and personal preferences from the collected information.

4. RESEARCH ON PROTECTION TECHNOLOGIES

4.1 Protection Against Specific Security Threats

Device access control safeguards users' private information by leveraging technologies including identity authentication, access control, and authorization. [8] Achieved group member key sharing via bilinear pairing mapping and developed a certificateless authentication protocol. [9] Lowered computational overhead through the design of an identity authentication protocol based on the Chinese Remainder Theorem, yet it lacked key confirmation and message integrity protection mechanisms. [10] Carried out an upgrade on the initial version of FairAccess, put forward the 2.0 framework, and refined the granularity of access control with the application of smart contracts.

Table 1: Comparison of Protection Schemes for Common Security Threats

Security Threats	Protection Technology	Reference	Scenario	Key Technologies	Security Analysis and Limitations
Access Security	Identity Authentication	[8][9]	Lightweight IoT	Bilinear Pairing, Chinese Remainder Theorem	Defends against replay attacks and forgery attacks, but lacks complete message integrity verification.
	Access Control	[10]	Small and Medium-sized Enterprises	Blockchain	Defends against rights spoofing, but has difficulty defining attribute rules.
Data Security	Privacy Protection	[11]	Industrial Internet	Federated Learning	compression rate improvement, without considering malicious node attacks.
	Homomorphic Encryption	[12]		Blockchain	Key management overhead is O(n2), with poor scalability.
Communi-cation Security	Physical Layer	[13]	IoT (UAVs, Smart Cities)	Clustering	Strong anti-interference capability, but complex signal environment reduces accuracy.
	Intrusion Detection	[14]		Signature, Anomaly Detection	Effectively identifies intrusions, but detection latency increases significantly under high load.
	Trust Evaluation	[15]	Internet of Vehicles	Federated Learning	Effectively evaluates node trustworthiness, but low efficiency in multi-node coordination and large overhead.

Data transmission security is mainly protected against various network attacks through encryption, intrusion detection, trust assessment, physical-layer technologies and other relevant methods. For instance, researchers in [11] proposed a privacy-preserving federated learning method that integrates differential privacy and adaptive compression, tailored for industrial edge computing environments. In [12], blockchain technology was incorporated to design a multi-key fully homomorphic encryption protocol specifically for privacy protection. The study in [13] developed an authentication scheme based on lightweight symmetric cryptography, which combines clustering and channel information to achieve mutual authentication between terminals and edge nodes. Meanwhile, [14] designed an intrusion detection system for MEC environments, leveraging the respective advantages of signature-based and anomaly-based detection mechanisms. For vehicle-road-cloud collaborative systems, the research in [15] realized node trust evaluation by adopting federated learning. All the schemes mentioned above are summarized in Table 1.

4.2 Protection Against Specific Security Threats

[16] proposed a Q-learning-based location privacy preservation scheme that can adapt to user requirements. [17] adopted differential privacy to obfuscate user location information and obtained the optimal decision based on the whale optimization algorithm. [18] employed a proxy forwarding mechanism to protect the location information of devices, and devised a privacy-preserving offloading scheme to preserve both location privacy and correlation privacy. [19] explored the privacy risks corresponding to diverse offloading preferences of edge nodes, adopted privacy entropy to measure the degree of privacy protection, and proposed an offloading scheme based on stochastic game theory. [20] took into account the protection of both location privacy and usage pattern privacy, and added the secure offloading rate constraint to the offloading target to realize energy-efficient offloading with minimal energy consumption. Table 2 provides a summary of the aforementioned studies.

Table 2: Comparison of Protection Schemes for Special Security Threats

Security Threats	Protection Technology	Reference	Scenario	Key Technologies	Security Analysis and Limitations
location privacy threats	Privacy Protection	[16]	Internet of Things (Multi-node Collaboration, Internet of Vehicles)	Q-learning	Dynamic optimization strategy, but slow convergence.
		[17]		Whale Optimization Algorithm, Differential Privacy	High privacy accuracy, but prone to local optima.
		[18]		Proxy Forwarding	Low deployment difficulty, but data delay in proxy forwarding.
		[19]		Stochastic Game Theory	Strong anti-interference, but complex game modeling.
Privacy Threats on Usage Patterns		[20]		Secure Offloading Rate	Improves secure offloading rate, but poor adaptability to heterogeneous nodes.

5. CHALLENGES AND PROSPECTS

5.1 Existing Challenges

Despite ongoing advancements in edge computing development, it still confronts prominent multi-dimensional challenges that hinder its large-scale application. For one thing, in complex environments, communication stability, anti-interference capability and network handover smoothness remain insufficient. The dynamic changes in network topology lead to high latency in traditional offloading schemes, which in turn result in unbalanced resource allocation. For another, end devices are limited by scarce resources and show considerable differences in their task resource requirements. Traditional encryption schemes generate high latency when applied to terminals with low computing power, failing to meet real-time demands.

Against this backdrop, balancing application costs and benefits has become a key consideration. Terminal devices suffer from limited battery life, and large-scale node deployment brings high operation and maintenance costs. At the same time, dynamic topology and heterogeneous resources in complex environments increase the difficulty of ensuring network reliability, which easily leads to unbalanced task allocation and directly impacts the overall stability of the system. Additionally, the lack of unified technical standards in the industry results in significant discrepancies between devices and technologies from different manufacturers. Inconsistent data formats, communication protocols and authentication standards create obstacles for cross-device and cross-domain collaboration.

5.2 Future Directions

1) Intelligent Computation Offloading Strategy

With machine learning and artificial intelligence algorithms, it can analyze task requirements of devices and network transmission capacity in time, thereby making accurate and optimal offloading decisions.

2) Efficient Communication

By utilizing new-generation communication technologies including 6G and quantum communication, a comprehensive and effective communication architecture is constructed. Combined with technologies including communication-sensing integration and intelligent reflecting surfaces, it addresses issues like signal occlusion and multipath fading in complex environments, and reduces signal loss and power consumption.

3) Trusted Collaborative Offloading

Blockchain technology is introduced to upload the interactive information of participants onto the chain, prevent malicious behaviors and data tampering, optimize cross-domain authentication mechanisms, establish collaborative incentive mechanisms, and study efficient consensus algorithms suitable for dynamic network environments.

4) Energy-Efficient

To address the issue of energy consumption, optimizing hardware design, control algorithms and task scheduling can effectively reduce energy usage in devices. For edge nodes, adopting energy-efficient architectures alongside

intelligent energy management strategies helps cut down their power consumption.

5) Lightweight Security

To address resource constraints in end devices, lightweight cryptographic algorithms are implemented to maintain security while optimizing system performance. Secure authentication and fine-grained data access control between terminals and edge nodes are achieved through attribute-based encryption and identity-based encryption schemes.

FUND PROJECT

Postgraduate Innovation Project of Qinghai Minzu University (09M2024009): Research on Blockchain-Based Identity Authentication in Edge Environments.

REFERENCES

[1] Lopez, P. G., Montresor, A., Epema, D., et al. (2015). Edge-centric computing: vision and challenges. *Computer Communication Review*, 45(5), 37-42. https://doi.org/10.1145/2831347.2831354
[2] Liu, H. (2021). Research on multi-workflow scheduling algorithm based on deep reinforcement learning under edge computing. Chongqing University. https://doi.org/10.27670/d.cnki.gcqdu.2021.001797
[3] Xu, J., Chen, L., Liu, K., et al. (2016). Designing security-aware incentives for computation offloading via device-to-device communication. https://doi.org/10.48550/arXiv.1611.03841
[4] Roman, R., Lopez, J., & Mambo, M. (2016). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78(PT.2), 680-698. https://doi.org/10.1016/j.future.2016.11.009
[5] Yi, S., Qin, Z., & Li, Q. (2015). Security and privacy issues of fog computing: A survey. In International Conference on Wireless Algorithms, Systems, and Applications (pp. 685–695). Springer International Publishing. https://doi.org/10.1007/978-3-319-21837-3_67
[6] Tadi, S., Kova, M., & Cokorilo, O. (2021). The application of drones in city logistics concepts. *Promet-Traffic & Transportation*, 33(3), 451-462. https://doi.org/10.7307/ptt.v33i3.3721
[7] Persiani, C. A. F., Sallazar, F. M., Inoue, R. S., et al. (2025). Drone-based fault recognition in power systems: A systematic review of intelligent methods. *Discover Applied Sciences*, 7(5), 1-19. https://doi.org/10.1007/s42452-025-06774-z
[8] Semal, B., Markantonakis, K., & Akram, R. N. (2018). A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. IEEE, 1-8. https://doi.org/10.1109/DASC.2018.8569730
[9] Lei, Y., Zeng, L., Li, Y. X., et al. (2021). A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access, 9, 53769-53785. https://doi.org/10.1109/ACCESS.2021.3070683
[10] Aafaf, O., Anas, et al. (2017). FairAccess: A new blockchain-based access control framework for the Internet of Things. *Security and Communication Networks*, 9(18). https://doi.org/10.1002/sec.1748
[11] Jiang, B., Li, J., Wang, H., et al. (2023). Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression. *IEEE Transactions on Industrial Informatics*, 19(2), 1136-1144. https://doi.org/10.1109/TII.2021.3131175
[12] Liao, J., Wang, H., & Wu, J. (2023). A multikey fully homomorphic encryption privacy protection protocol based on blockchain for edge computing system. *Concurrency & Computation: Practice & Experience*, 35(4). https://doi.org/10.1002/cpe.7539
[13] Chen, Y., Wen, H., Wu, J., et al. (2019). Clustering based physical-layer authentication in edge computing systems with asymmetric resources. *Sensors*, 19(8), 1926. https://doi.org/10.3390/s19081926
[14] Alsubhi, K. (2024). A secured intrusion detection system for mobile edge computing. *Applied Sciences*, 14(4), 2076-3417.
[15] Wang, D., Yi, Y., Yan, S., et al. (2023). A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2022.103013
[16] Liu, X. H., Yang, C. Y., Xu, R. Z., & Nian, J. C. (2023). Location privacy protection for multi-access edge computing in smart grid based on reinforcement learning. *Electric Power Information and Communication Technology*, 21(1), 47-53.
[17] Liu, Z., Wang, J., Gao, Z., et al. (2023). Privacy-preserving edge computing offloading scheme based on whale optimization algorithm. *Journal of Supercomputing*. https://doi.org/10.1007/s11227-022-04756-1

[18] Yu, H., Liu, J., Hu, C., et al. (2023). Privacy-preserving task offloading strategies in MEC. *Sensors*, 23(1), 95. https://doi.org/10.3390/s23010095
[19] Wu, G., Chen, X., & Shen, Y. S. (2024). Privacy-preserving offloading scheme in multi-access mobile edge computing based on MADRL. *Journal of Parallel and Distributed Computing*, 183(Jan.), 104775. https://doi.org/10.1016/j.jpdc.2023.104775
[20] Sun, Y., Li, N., & Tao, X. (2021). Privacy preserved secure offloading in the multi-access edge computing network. In 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 1-6). https://doi.org/10.1109/WCNCW49093.2021.9419987