Homework 1

Geng Tian
Department of Computer Science and Engineering
Southern University of Science and Technology
Shenzhen, China
12332463@mail.sustech.edu.cn

***Abstract*—This is the paper I chose: [1] [2]. The initial article explores security and privacy concerns posed by technologies like edge storage and edge computing in 6G networks. The second article discusses a popular 6G network architecture discussed in the first article, which is a specific network architecture that can be applied to edge servers. Building upon the first article, this paper presents a comprehensive discussion on the background of application edge servers in 6G networks, the research motivation, objectives of edge server security research, as well as the existing main issues and solutions, alongside some open matters. The primary goal is to provide a complete overview of the problems and feasible solutions associated with edge computing and edge storage in 6G network systems.**

***Index Terms*—Security, privacy, edge intelligence, edge computing, edge caching, 6G, security threats**

I. Background

Today, we are living in the 5G network era, and many everyday devices are connected to the Internet. It is predicted that by 2023, there will be approximately 10 billion networked devices worldwide [3]. According to statistics, these networked devices are expected to generate around 850 zettabytes of traffic in 2021 [4]. These numbers will continue to increase in the future.

Research and development of 6G has begun and many communication equipment vendors around the world are starting to develop 6G communication equipment. Using 6G networks, operators will be able to offer greater bandwidth and lower communication latency.

With the rapid development of 6G, various network system structures have been proposed to support high-speed information transmission. An instance of such a structure is the Space-Air-Ground-Sea Integrated Network (SAGSIN), which is an amalgamated network architecture incorporating space, air, ground and sea network systems to provide users with high-quality network access services.

To achieve low-latency, high-bandwidth communications, 6G operators will need to adopt edge computing and edge storage approaches. Both approaches respond to users by deploying a large number of servers at the edge of the network. This pattern can support latency-sensitive applications very well [5] [6].

Edge computing can be utilized in the Space-Air-Ground-Sea Integrated Network (SAGSIN). As a form of distributed computing, it permits the expansion of cloud computing functions to the edge nodes of the network, which can greatly reduce the burden on the central server. Moreover, edge storage is widespread within SAGSIN. Within the context of SAGSIN, edge computing and edge storage provide a diverse range of user resources situated at the network's periphery. This feature significantly improves efficiency, reduces delay, and ultimately enhances the user experience [2].

The Space-Air-Ground-Sea Integrated Network(SAGSIN) can be deployed in a wide array of regions. Besides, mobile computing and mobile storage functions are flexible and adaptable depending on the network system's location. Mobile computing and storage can be employed across various locations within SAGSIN, including base stations, drones, maritime buoys, and more. This comprehensive deployment enables SAGSIN to provide seamless network services to users in diverse locations, aided by the 6G networks.

However, the deployment of edge computing and edge storage gives rise to several security risks. These risks impede the widespread commercial use of 6G networks. Moreover, the issues discussed are not limited to SAGSIN, which is just one example.

Many network architectures pose security risks to users when it comes to edge computing, edge storage, and related businesses. This compromise of privacy has been analyzed in multiple studies, yet some unanswered questions still remain.

My research area is focused on edge computing, wherein an attack on a user's data can have repercussions on the entire system. For instance, if the user's data is polluted with noise by a network tool, the accuracy of the trained model is reduced. To address this, a considerable amount of research has been focused on modifying neural network training logic to enable edge computing systems to tolerate noisy user data [7]. In addition to the aforementioned research, my selection paper proposes an alternative solution. Within the framework of the 6G network, enhancing the security of the edge computing system can increase the reliability of user data. This, in turn, improves the accuracy of the comprehensive model. The following discussion will focus on how to solve the security and privacy issues of 6G network systems with edge servers.

II. Research Motivation

A. Edge servers play an important role in 6G networks

The architecture of 6G networks differs from that of previous networks in that it relies on large-scale edge computing and edge storage systems to enable low latency, high-

bandwidth communication for users. If the central server continues to bear the majority of the computing and storage load, as in previous networks, the network system is unable to deliver reliable, high-speed network connections.

During edge computing processes, the possibility of encountering network attacks is high [8], which can lead to damage to data or models. Furthermore, it is quite simple to invade nodes where data is stored in edge storage, which endangers the confidentiality of user data. Therefore, there is a need to investigate and research adequate measures to combat these risks of edge computing and storage.

B. Lack of investigation of edge computing security issues

Many studies regarding computer network security fail to address the implications of edge computing and edge storage. Instead, they focus solely on the security of the network system architecture [2] [9] [10] [11].

Within edge computing research, experts predominantly hold the belief that edge computing can enhance network security [12] [13] [14]. This is due to the technology's ability to better safeguard user privacy, and its decentralized nature, which helps prevent large-scale network intrusion. There is limited literature available on the topic of edge computing and edge storage being vulnerable to external attacks.

Edge computing aims to provide users with computing resources in close proximity, thereby enhancing network efficiency. However, it also poses several vulnerabilities in the system, which can be exploited to breach security. Hence, bolstering the security of edge computing is imperative to avert diverse network assaults via edge nodes, which jeopardize the security of the network and users' privacy.

Just like edge computing, edge storage is fraught with several security hazards regarding data security and user privacy. Since data is classified in disparate nodes, edge storage necessitates more data transfer than centralized storage systems. The process of transmitting data is vulnerable to network attacks, making it crucial to prioritize security and protect user privacy.

III. RESEARCH OBJECTIVES

A. Secure edge servers

Edge servers that provide edge computing and storage services may be vulnerable to numerous security threats, including network attacks and data breaches. With the emergence of 6G networks, many new network systems containing edge nodes need to be supported, which may have undetected weaknesses and increase the chances of attacks against users. The edge node hosting the edge server often lacks the same computing and storage resources as the central server. This, however, enhances the security of the system. The reason being that several robust algorithms, which can protect server security, necessitate substantial computing resources. Furthermore, as the usage of 6G network evolves, numerous novel features will be made available by edge servers to users. These functions have the potential to intensify the pre-existing vulnerabilities, thereby causing grave harm to the edge nodes in case of a cyber attack. Hence, it is imperative to establish customized security measures for edge servers.

The Space-Air-Ground-Sea Integrated Network (SAGSIN) is susceptible to risks when edge computing and edge storage are combined [2]. The SAGSIN system has a broad delivery range, with edge nodes situated on land, sea, air, and other locations. These nodes have various types that differ significantly, which amplifies the inherent security risks of edge nodes and increases their susceptibility to attacks. One of the research objectives is to protect edge servers from attacks by strengthening security protection.

B. Balance network security and load

The purpose of introducing edge computing and edge storage in 6G network is to speed up the speed and improve the efficiency of the network. Therefore, while solving the security problem, the speed and efficiency of the network should not be excessively sacrificed, and the balance between network security and network speed should be found. The points that need to be weighed can be roughly divided into the following four aspects:

First, the quality of service (QoS) may be affected by system security: the use of powerful security algorithms demands significant computing and storage resources, and if these functions are carried out at the nodes of the system, it may impair its normal functioning, thereby leading to a reduction in the quality of service. When ensuring the security of the edge server, it is crucial to maintain high overall service quality of the system. Otherwise, the introduction of the edge server would not be warranted [15].

Additionally, global resource management can be impacted by system security, as edge servers typically have restricted resources that can be allocated to security protection mechanisms. Ensuring the reasonable utilization of resources and safeguarding edge servers without compromising global resource management is a critical area of research. If the edge server is at full capacity, it may be necessary to reduce resource-intensive security mechanisms.

Third, the introduction of edge computing and edge storage functions in 6G networks can significantly enhance network performance; however, the security of edge servers must not be prioritized over network performance. Network performance is crucial to the 6G network system and should be maintained while ensuring edge server security and user privacy.

Fourth, system security may also impact network reliability. The initial aim of enhancing network security is to improve the reliability of the entire network system. In edge computing and edge storage, the dependability of the network is of utmost significance because the decentralized approach heavily relies on network transmission, and a decrease in dependability is likely to lead to the network system's failure. Consequently, network reliability must be ensured.

IV. MAIN CHALLENGES AND EXISTING SOLUTIONS

A. Main challenges

Security attacks at the network's edge pose significant challenges to 6G network systems. Numerous types of attacks exist. This summary of such attacks includes the following: 1)Denial of Service (DoS) attacks. The number of end devices connected to the Internet has surged in recent years, primarily due to the fast growth of applications such as autonomous driving. However, most of these devices are vulnerable because of limited computing and communication resources [11]. These devices are vulnerable to control by malicious users, who use them to launch distributed denial of service (DDoS) attacks. These attacks involve creating a large number of computing tasks that consume the resources of edge servers. Moreover, a DoS attack could also be directed towards the terminal device, disrupting its service [16]. Therefore, Dos attack can be a significant challenge in this context. 2)A range of emerging web applications, including smart homes and smart healthcare, are swiftly developing. These technologies empower users to remotely control and manage devices in real time with ease. However, these services pose the potential risk of exposing users' personal information online. This can lead to malware attacks and compromise users' data security [17]. Furthermore, malware can command computing resources from end devices and edge servers to carry out unauthorized tasks, including cryptocurrency mining. As a result, legitimate users may face the risk of exorbitant electricity bills. Due to the wide variety of operating systems in use and the varied intentions of malware operators, safeguarding edge systems from malware attacks can be an arduous undertaking. 3)The act of providing false data to edge servers in an effort to hinder the training or operation of an AI model is known as a data contamination attack. Such attacks, carried out by unauthorized users during the training phase, can cause the model to be trained poorly or incorrectly [18]. During operation, deep learning models may encounter contaminated inputs, leading to erroneous output and consequent network performance degradation. Given that AI has already found extensive implementation in edge computing and storage, data contamination attacks can compromise these services.

On edge servers, safeguarding data privacy poses a significant challenge. Three primary threats to data privacy exist: 1)Firstly, the presence of eavesdroppers that have been a considerable threat to privacy. The connectivity of numerous devices to the network system is on the rise, with the prevalence of 6G networks, resulting in increased transmission of information. The transmission of information often involves a considerable amount of data that is privacy-sensitive, including but not limited to personal information and trade secrets. If the listener gains access to the data, it can be used for illegal purposes. As most of the devices connected to network systems lack sufficient computing resources, it becomes difficult to use efficient yet complex encryption algorithms to protect the data [19]. Eavesdroppers are typically difficult to detect within the system since they do not disrupt normal communication processes. This presents numerous challenges for ensuring the privacy and security of edge nodes. 2)Additionally, while modifying the storage method of storage servers can improve privacy protection against data access abuses, the sharing mechanism of edge servers remains a significant obstacle to privacy protection. Third-party applications responsible for providing various services can utilize network virtualization technology in order to access and handle stored data. However, it is often the case that these applications request and access significantly more data from edge servers than is actually required, thereby infringing on the data privacy of users. Additionally, third-party application vulnerabilities can lead to tampering with data on edge servers, resulting in abnormal termination of other applications due to shared data. 3) The resources of edge servers for computing and storage are very limited, which may hinder the provision of high-quality 6G Internet services to users. 6G networks frequently engage different users or servers to assist with data storage and processing for better service. However, not all users or servers participating are dependable, which makes privacy protection more challenging. When assisting with data storage and processing, untrustworthy users or servers may feign reliability, whilst surreptitiously extracting data from the server, thus violating user privacy [20] [21].

B. Existing solutions

Federated Learning (FL) represents an essential technology for 6G network systems, as it enables networks to tackle various challenges that are complex, dynamic, and diverse, whilst improving user privacy. FL adopts a distributed training framework, comprising a central server and numerous distributed participants. Every participant leverages a designated subset of data to train a local AI model, with the central server responsible for aggregating these local models to generate a global model. This approach exclusively permits local storage and use of personal data, without uploading any personal information on the server, thereby enhancing data security and considerably reducing communication overheads [22]. Federated learning exhibits diverse utilizations in 6G edge services, comprising of Distributed Intrusion Detection Systems (IDS), private data handling, content caching, and provision of suggestions.

Blockchain technology seeks to address security issues present in conventional centralized control systems [12]. In the case of blockchain-based systems, several users manage the blocks employed to document user transactions, as opposed to a singular central server. Furthermore, newly created blocks update recent transactions, instead of replacing established blocks. As well as transaction data, the value of the previous block and the latest timestamp are also recorded. As a consequence, users can independently trace and authenticate information on each block without the requirement of a third party or central controller, and at low cost. Additionally, managing permissions to access data, generate blocks, and verify records is feasible to guarantee data security and privacy.

V. OPEN PROBLEMS

A. Emerging Edge Network Architecture and Infrastructure

The majority of the existing Radio Access Network (RAN) infrastructure is comprised of proprietary hardware, leading to restricted implementation of new technologies and services. Researchers from both industry and academia have explored novel access network infrastructures and architectures to enhance network flexibility and openness, enabling the provision of services at the network edge such as edge computing, caching, and intelligence. O-RAN, an open radio access network architecture, is being implemented on both generic and proprietary hardware, providing a promising direction for enhancing the edge of 6G networks [23].

B. Improved Distributed Security and Privacy Protection

Federated learning and blockchain have the potential to enhance the effectiveness and security of edge servers. The crucial aspect of this approach is to ensure the reliability of participants in FL, as untrustworthy members can cause data breaches or compromise system security. Blockchain presents the opportunity for security protection and digital verification, although these domains are still in the theoretical research phase. Blockchain technology requires significant energy consumption and time commitment [24], necessitating further research to address these issues.

C. Adaptive, Multi-Level, and Multi-Tiered Security and Privacy Protection

Currently, network systems present a diverse range of security mechanisms at both software and hardware levels [25]. The implementation of the 6G system will offer more opportunities for the application of artificial intelligence technology in security. By using artificial intelligence, potential threats can be forecasted, and the network system can then adjust its security policies to suit accordingly. In the practical operation of the network system, achieving the utmost service quality necessitates adjusting the security service scheme subjected to changes in the operating system, device status, and other relevant parameters. Consequently, the preparation of diverse security configurations onto the network system and adaptive provision of security services with the guidance of artificial intelligence are pivotal trajectories for network system security. This adaptive security system can aid in addressing the intricate and evolving network security concerns.

D. Complex Integration of Edge Computing, Edge Caching, and Edge Intelligence

After the integration of 6G service into the network system, the responsibility of the infrastructure of the network system expands beyond mere data transmission. With the emergence of edge computing, edge storage, and intelligence, they represent a new focal point of the network system. The infrastructure of the 6G network must assume responsibility for integrating these three tasks, enabling them to work in collaboration. The optimization level of these three technologies will significantly impact the performance of the user experience and the stability of the network infrastructure.

E. Joint Optimization of Security, Privacy, and QoS

After the incorporation of 6G into the network system, the network must continually weigh tradeoffs between security, privacy, and QoS [26] [27]. These three metrics jointly indicate the quality of a network system; therefore, the 6G network system should strive to optimize all three indicators instead of compromising some of them. Determining how the network system can achieve a balance between security, privacy, and QoS is a crucial area of investigation for future research.

F. Lightweight AI-Based Security and Privacy Protection

With the advancement of 6G technology, the network system's edge nodes necessitate the assistance of artificial intelligence [28] [29]. The foremost AI technique is machine learning, which demands abundant computing and memory resources that are frequently arduous to procure in edge servers. Consequently, researchers must create more featherweight AI techniques, which can be employed in network system edge nodes.

These lightweight AI techniques must exhibit uncomplicated performance. Many conventional AI algorithms, such as genetic algorithms, may be useful in addressing some of the challenges that edge servers are confronted with. Though these AI algorithms cannot attain identical high precision as machine learning algorithms, they demand merely a small quantity of memory and computing resources to execute.

REFERENCES

[1] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6g network edge: A survey," *IEEE Communications Surveys & Tutorials*, 2023.

[2] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 53–87, 2021.

[3] "Cisco annual internet report (2018–2023) white paper." [Online]. Accessed: Oct. 2021. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[4] D. Xu, T. Li, Y. Li, X. Su, S. Tarkoma, T. Jiang, J. Crowcroft, and P. Hui, "Edge intelligence: Empowering intelligence to the edge of network," *Proceedings of the IEEE*, vol. 109, no. 11, pp. 1778–1837, 2021.

[5] H. Guo, X. Zhou, Y. Wang, and J. Liu, "Achieve load balancing in multi-uav edge computing iot networks: A dynamic entry and exit mechanism," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18725–18736, 2022.

[6] C. Li, H. Zhao, Y. Zhao, B. Zhang, and C. Li, "Joint transcoding-and recommending-based video caching at network edges," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4928–4937, 2021.

[7] J. Xu, Z. Chen, T. Q. Quek, and K. F. E. Chong, "Fedcorr: Multi-stage federated learning for label noise correction," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 10184–10193, 2022.

[8] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.

[9] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[10] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6g: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2694–2724, 2020.

[11] Z. M. Fadlullah, B. Mao, and N. Kato, "Balancing qos and security in the edge: Existing practices, challenges, and 6g opportunities with machine learning," *IEEE Communications Surveys & Tutorials*, 2022.

[12] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable iiot critical infrastructures in industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300–2317, 2020.

[13] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge computing and its convergence with blockchain in 5g and beyond: Security, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 205340–205373, 2020.

[14] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12806–12825, 2021.

[15] B. Mao, Y. Kawamoto, and N. Kato, "Ai-based joint optimization of qos and security for 6g energy harvesting internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7032–7042, 2020.

[16] R. Swami, M. Dave, and V. Ranga, "Software-defined networking-based ddos defense mechanisms," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–36, 2019.

[17] K. Suzaki, A. Tsukamoto, A. Green, and M. Mannan, "Reboot-oriented iot: Life cycle management in trusted execution environment for disposable iot devices," in *Annual Computer Security Applications Conference*, pp. 428–441, 2020.

[18] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[19] S. Zhang, W. Sun, J. Liu, and K. Nei, "Physical layer security in large–scale probabilistic caching: Analysis and optimization," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1484–1487, 2019.

[20] B. Wu, K. Xu, Q. Li, S. Ren, Z. Liu, and Z. Zhang, "Toward blockchain-powered trusted collaborative services for edge-centric networks," *IEEE network*, vol. 34, no. 2, pp. 30–36, 2020.

[21] Q. Xu, Z. Su, and Q. Yang, "Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1098–1110, 2019.

[22] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[23] M. Polese, L. Bonati, S. D'oro, S. Basagni, and T. Melodia, "Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Communications Surveys & Tutorials*, 2023.

[24] T. G. Nguyen, T. V. Phan, D. T. Hoang, T. N. Nguyen, and C. So-In, "Federated deep reinforcement learning for traffic monitoring in sdn-based iot networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 4, pp. 1048–1065, 2021.

[25] B. Mao, Y. Kawamoto, J. Liu, and N. Kato, "Harvesting and threat aware security configuration strategy for ieee 802.15. 4 based iot networks," *IEEE communications letters*, vol. 23, no. 11, pp. 2130–2134, 2019.

[26] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5g mobile edge computing environment," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081–7093, 2019.

[27] K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1685–1696, 2021.

[28] S. Xu, Y. Qian, and R. Q. Hu, "Data-driven network intelligence for anomaly detection," *IEEE Network*, vol. 33, no. 3, pp. 88–95, 2019.

[29] S. Xu, Y. Qian, and R. Q. Hu, "Data-driven edge intelligence for robust network anomaly detection," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 1481–1492, 2019.