AI-BASED SECURITY ENHANCEMENT AND PERSONAL INFORMATION PROTECTION TECHNIQUES INHERITED FROM 6G NETWORKS

Kwang-Man Ko, Chul-Long Kim, Jun-Seop Lim,
Seong-Won Kim, and Byung-Suk Seo

Department of Computer Engineering, Sangji University,
Won-Ju, Republic of Korea

ABSTRACT

As the realization of digital transformation expected with 5G networks has already begun and continue to evolve over this decade, the 6G communication era envisions how humans will interact with the digital virtual worlds beyond 2030. The security mechanisms designed for 5G using the concepts of SDN and NFV should be further improved to cater to the security demands in 6G networks. When 6G networks are harmonizing the concepts of SDN, NFV, and AI in an integrated environment to provide the necessary services, the system-level differences between 5G and 6G would introduce new security threats and privacy concerns. This paper aims to identify and systematically analyze new security threats and privacy concerns of 5G technologies inherited from 6G networks. The corresponding 6G-specific defenses will also be investigated.

KEYWORDS

5G Networks, 6G Networks, Security and Privacy, Machine Learning.

1. INTRODUCTION

The 6G Networks(6G) communication era envisions how humans will interact with the digital virtual worlds beyond 2030. Future networks must possess novel technologies that enable the digital virtual worlds with connected intelligence, to address the communication and networking challenges beyond 2030. 6G rely on AI to enable fully autonomous networks[1]. In order to lead the 6G communication market, core technologies are being developed competitively, centering on the United States, Korea, China, Japan, and the European Union (EU). 6G technology aims to support services of up to 1Tbps (terabit per second, 1Tbps = 1000Gbps) by implementing a network that is about 50 times faster than the maximum speed of 5G networks (5G) of 20Gbps. In addition, the delay time, which is the reaction speed of the network, is 0.1 millisecond, which is one tenth of 5G, and has the characteristic of using the terahertz (THz) band.

Until now, various security issues have been continuously raised in 5G. Even in the future 6G network era, more intelligent and advanced technology development is expected for the development of technologies and tools related to security, trust, and privacy based on Artificial Intelligence(AI). Therefore, attacks on AI systems, especially Machine Learning (ML) systems, will catastrophic affect 6G networks. Such as poisoning attacks, data injection, data manipulation, logic corruption, model evasion, model inversion, model extraction, and

David C. Wyld et al. (Eds): IoTE, CNDC, ACITY, DPPR, AIAA, NLPTA, WEST, ICSS -2023
pp. 261-269, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.132220

membership inference attacks are potential security threats against ML systems. The collection of more features allows AI systems to perform better. Attacks on collected data and the unintended use of private data lead to privacy issues as the data processing is usually not visible to the users[2].

AI-enabled security and privacy provision are core part of 6G systems. 6G achieves connected intelligence via AI-enabled functions, especially with ML systems that are subject to various threats. Specially, poisoning attacks influence the learning phase of a ML system, which lead the model to learn inaccurately. Multi-connectivity, mesh networks with tiny cells in 6G allow simultaneous communication for devices via multiple base stations[3]. Edge-based ML models could be used for dynamic detection of privacy-preserving routes, rank them, and allow devices to transfer data via privacy-preserving routes based on the ranking. federated learning keeps data in the users proximity compared to cloud-based learning to enhance data privacy and location privacy[3]. The 6G subnetwork level AI allows better privacy within the subnetwork and share only the learned intelligence outside to minimize privacy risks. Confining data within the network is suitable for applications like in-body networks. With the vast number of applications in 6G and the massive data collection to feed ML/DL models, users would prefer different privacy levels on different applications. AI-based service-oriented privacy-preserving policy updates are a potential way to enhance privacy in automated 6G networks[3].

Inspired by this need, this study aims to conduct a thorough study on the emerging security and privacy issues in 6G and on how to address these issues. First, 5G network softwareization is expected to continue with security issues in 6G along with functional and performance improvements. Therefore, research to solve these issues based on artificial intelligence is needed. Second, security issues related to SDN, NFV, MEC, etc., which seek to improve 5G functions and performance through software, are expected to become more intelligent and advanced in 6G. Therefore, even in 6G, it is required to develop a technology that can overcome security issues in this area. Third, in a 6G IoE edge AI environment where billions of heterogeneous IoT devices are hyper-connected, a security technology that can overcome advanced intelligent attacks against IoE edge AI with limited computing resources is required. In addition, it is required to develop technology that can prevent damage to large-capacity collected data and protect sensitive personal information.

The security mechanisms designed for 5G using the concepts of SDN and NFV should be further improved to cater to the security demands in 6G networks. When 6G are harmonizing the concepts of SDN, NFV, and AI in an integrated environment to provide the necessary services, the system-level differences between 5G and 6G would introduce new security threats and privacy concerns. In this paper, we aim to identify and systematically analyse new security threats and privacy concerns of 5G technologies inherited from 6G and the corresponding 6G specific defences will also be investigated.

The remainder of the article is organized as follows. In the next section, the background and research trends related to 6G security and privacy. In chapter 3, we addressed our research approaches regarding softwarization security issues of 5G technologies inherited to 6G network. And, we describes the AI-enabled illegal traffic detection approaches in 6G network. In chapter 4, we describes the conclusion of this paper and the direction of future research.

2. RESEARCH BACKGROUNDS

2.1. Backgrounds

As the realization of digital transformation expected with 5G has already begun and continue to evolve over this decade, the 6G communication era envisions how humans will interact with the digital virtual worlds beyond 2030. 6G technology is being developed closely related to AI in the fields of federated learning, IoE, compressive sensing, post-quantum computing, and intelligent security. In addition, the standardization of 6G technology is aimed at full-scale commercialization after 2028. Up to now, the core technology and details of 6G are in the beginning stage, but the US, China, Korea, Finland, and Japan are actively conducting future research in each expected part and detailed area. Beyond 2030 wireless applications will demand much higher data rates, extremely low end-to-end latency, extremely high end-to-end reliability. Moreover, 6G networks will comprise a collection of heterogeneous dense networks embedded with connected intelligence and utilize hyper-connected cloudification. Service provision for extreme requirements with complex 6G requires sophisticated security mechanisms. The security mechanisms designed for 5G using the concepts of SDN and NFV should be further improved to cater to the security demands in 6G [5,6,7].

The end-to-end automation of future networks demands proactive threats discovery, intelligent mitigation techniques, and self-sustaining networks in 6G. Hence, the end-to-end security design leveraging AI techniques is essential to autonomously identify and respond to potential threats based on network anomalies rather than cryptographic methods. Network softwarization technologies are still applicable for 6G systems, the security issues associated with SDN and NFV would remain in 6G. Additionally, MEC in 6G is subject to physical security threats, Distributed Denial of Service (DDoS), and man-in-the-middle attacks [8]. Potential attacks for network slicing are DoS attacks and data theft via compromised slices [9]. Attacks on network softwarization fail the 6G network from achieving the promised dynamicity and automation. 6G envisions the realization of the IoE, a collection of billions of heterogeneous devices. Key distribution and management functions are highly inefficient in such a massive network [10]. The resource constrained IoT devices cannot afford complicated cryptography to maintain strong security [11], making them a primary target of the attackers. These devices can be compromised and potentially used to initiate attacks. Data collection by hyper-connected IoE to serve 6G applications raises privacy issues. Data theft by exploiting resource constrained IoT devices will affect data privacy, location privacy, and identity privacy. The present security mechanisms based on asymmetric key cryptography are vulnerable against quantum computer-based attacks as the 6G era will mark the presence of quantum computers. Thus, the 5G communications enabled with public key cryptography may be no longer secure without quantum-safe cryptographic algorithms [12]. In 6G, which aims to implement autonomous networks based on AI, attacks on AI models are expected to have a serious impact. Therefore, defences against poising attacks, data injection, model evasion, model reversal, model extraction and member reasoning attacks, etc., would become increasingly important.

2.2. State-of-Art Related Works

Multilayered intrusion detection and prevention using deep reinforcement learning and Deep Neural Networks (DNN) is viable in SDN/NFV-enabled networks [13]. They effectively defend IP spoofing attack, flow table overloading attack, DDoS attack, control plane saturation attack, and host location hijacking attack compared to several conventional approaches. ML approaches, such as Decision Trees and Random Forest, are also proved useful for detecting DDoS attacks in SDN environments due to their short processing time and accuracy, respectively [14]. ML-based

adaptive security approaches are effective against attacks on SDN/NFV as the 6G networks expect dynamic placement of virtual functions ed network. Hence, rule-based detection systems are ineffective. On-device resource limitations, the difficulty of key management in massive scale heterogeneous networks, the vast amount of device data make the conventional authentication/authorization systems insufficient for adequately securing large-scale IoT. Anomaly-based intrusion detection systems detect malicious packets based on their behavior [15]. In 6G networks, learning based detection systems could utilize various features of the data as the input; therefore, they are suitable for detecting zero-day attacks. The use of communication link attributes and user behaviours with machine learning for authentication and authorization [16, 17] is a better approach for resource constrained devices. The sub-networks in 6G, which can be considered an expansion of local 5G networks beyond vertical domains, can benefit from learning-based security techniques within the sub-network and between different sub-networks. ML-based algorithms deployed at the perimeter can capture the behaviour of other sub-networks and detect malicious traffic. To avoid poor communication efficiency, a sub-network can share only the learned security intelligence with others [18]. Nevertheless, a dedicated sub-network can use the shared intelligence, feed it into its ML models, determine the malicious traffic of other networks, and apply dynamic policies.

2.3. Research Motivations and Objectives

The security mechanisms designed for 5G using the concepts of SDN and NFV should be further improved to cater to the security demands in 6G. As 6G moves toward THz spectrum with much higher bandwidth, more densification and cloudification for a hyper connected world by joining billions of devices and nodes with global reach for terrestrial, ocean and space, automated security utilizing the concepts of security function softwarization and virtualization, and machine learning will be inevitable. To eliminate constraints in existing and evolving 5G networks security, security systems using the existing concepts of SDN and NFV must be further improved with embedding intelligence for dynamicity to match the needs of 6G security. In this vain, intelligent security functions in containerized VNF box will monitor traffic in 6G residing in gateways to scan the traffic using continuous deep learning on a packet/byte level and applying machine learning to enforce policies, detect, contain, mitigate, and prevent threats or active attacks. Security functions using container technology offers better utilization rates, less storage requirements, enhanced security, and faster reboot time. Containers will be grouped into Pods, each Pod consisting of multiple containers on a single machine, with security service functions and providing availability through scaling up or down. The advances in cloud computing such as edge and fog computing will be used to maintain and deploy security functions (security VNFs) in different network perimeters as the use arises through proactive decision-making using machine learning. Building on the concepts of SDN, global resource visibility and event monitoring, with synchronized network security policies among different stakeholders, and programmable APIs, network abstractions will be used to ensure end-to-end network security. 6G networks will harmonize the concepts of SDN, NFV, and AI in an integrated environment not only to provide the necessary service, but also to ensure end-to-end network security. Programmable interfaces on programmable forwarding plane will enable deploying softwarized security functions much like VNFs in any network perimeter or instance in a virtual environment using AI not only proactively discover threats, but also to initiate security function transfer from point-to-point throughout the network. Automated, zero touch and zero trust security where zero trust for all North-South (N-S outbound/inbound traffic from/to data center) and East-West (E-W form container to another) cloud traffic must be checked with AI based ML for threat detection, prevention, and containment where the network can be treated as a giant firewall that integrates the flowing security functions.

When 6G networks are harmonizing the concepts of SDN, NFV, and AI in an integrated environment to provide the necessary services, the system-level differences between 5G and 6G would introduce new security threats and privacy concerns. This paper aims to identify and systematically analyse these new security threats and privacy concerns. The corresponding 6G-specific defenses will also be investigated.

3. AI-BASED SECURITY ENHANCEMENT AND PERSONAL INFORMATION PROTECTION TECHNIQUES ON 5G NETWORKS

3.1. Security Issues of 5G Networks

Network softwarization technologies in 5G such as SDN, NFV, Multi-access Edge Computing (MEC), and network slicing are still applicable for 6G systems. Thus, their security issues would remain in 6G. SDN related prominent security issues are attacks on SDN controller, attacks on northbound and southbound interfaces, inherent vulnerabilities of platforms used to deploy SDN controllers/applications. NFV related security issues are attacks targeting Virtual Machines(VM), Virtual Network Functions(VNF), hypervisor, VNF manager, NFV orchestrator. Due to the massively distributed nature of 6G systems, MEC in 6G is subjected to physical security threats, DDoS, man-in-the-middle attacks. Potential attacks for network slicing are DDoS attacks, information theft via compromised slices. Although 6G network architectures are not completely immunized from the above-mentioned attacks, the newly added ML/DL capabilities in 6G networks provide exciting new opportunities to detect and defend against these attacks. How to leverage the new ML/DL capabilities for security purposes is an important problem which is still under investigated.

In order to properly leverage the new ML/DL capabilities for security purposes, the data characteristics of the vulnerabilities and attacks inherited from 5G should be firstly studied. To this end, we examine attack vulnerability detection and defence techniques for ML/DL-based SDN. In this process, we study network attack detection and mitigation techniques for SDN based on ML such as decision trees and random forests, and detection and effective mitigation techniques for IP spoofing, flow table overload, and DDoS attacks based on deep reinforcement learning and DNN. And, ML/DL-based 6G network vulnerability detection and defence technology are considered to detect and prevent attacks expected in 6G networks. In particular, terminal devices such as hardware and software manipulation attacks, physical attacks that access physical devices, false data injection attacks that threaten moving data, data tampering attacks, man-in-the-middle attacks, and DDoS attacks develop attack detection and mitigation technology. Finally, through R-threat insight research that extracts relationships between security vulnerabilities, we develop attack detection and mitigation technologies by quickly and accurately checking threats and tracking them.

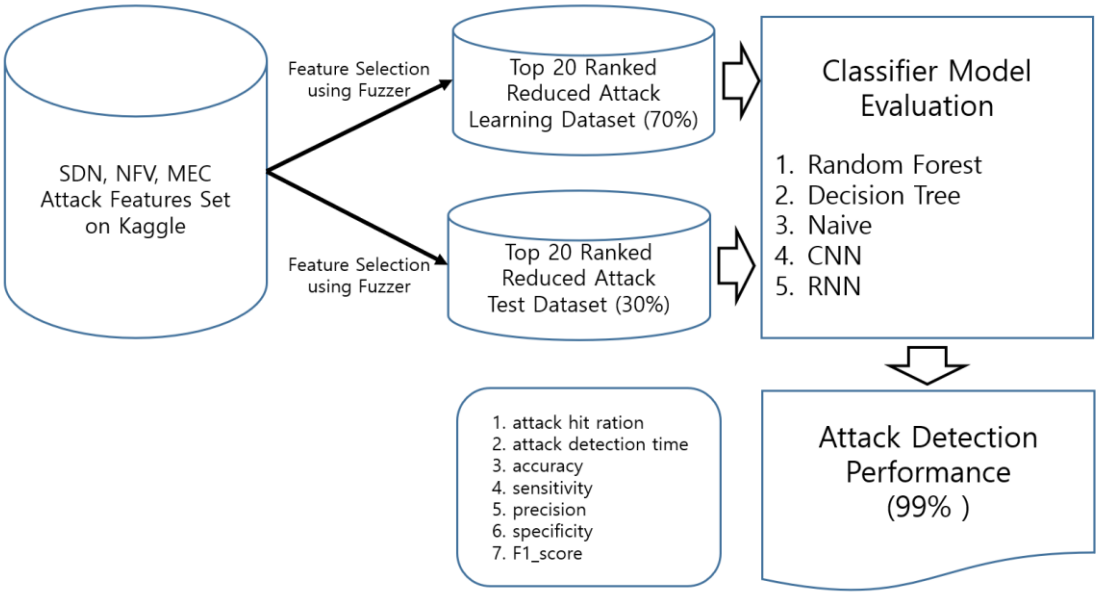

Figure 1. Structure of SDN, NFV, MEC Attack Detection Model

6G achieves connected intelligence via AI-enabled functions, especially with ML systems. We primarily utilized Kaggle to obtain reliable and diverse 6G threat data sets. For known attacks against 6G, fuzzing is used to identify each attack and collect the necessary data sets suitable for learning. In this way, the data can be automatically labeled by the fuzzer. Once the datasets are generated, we can train DNN models to detect attacks against 6G. In this way, we do not need to extract the features of such attacks. Through this, we could save a large amount of manual effort and increase the reliability and precision of the data. The DNN model completed through the proposed study is verified by applying it to the AI-enabled 6G smart factory sub-network and AI-enabled 6G i-transportation sub-network virtual environment. Through experiments, we evaluate effectiveness of the trained DNN models in detecting. In addition, we evaluated the model robustness against poisoning attacks, adversarial attacks, and relevant privacy threats. Finally, we quantitatively analyse the balance between the increased defense and performance degradation with our proposed mechanisms and model.

3.2. AI-enabled Detection of Illegal Traffic in 6G NETWORKS

6G envisions the realization of the Internet of Everything (IoE), a collection of billions of heterogeneous devices. The fundamental device security model relying on SIM cards is not a practical deployment for IoE in 6G, especially with the small form factor devices such as in-body sensors. Key distribution and management functions are highly inefficient in such a massive network. The resource-constrained IoT devices cannot afford complicated cryptography to maintain strong security, making them a primary target of the attackers. These devices can be compromised and potentially used to initiate attacks. Data theft by exploiting resource-constrained IoT devices will affect data privacy, location privacy, and identity privacy. When the attacker is using compromised devices to launch privacy and adversarial attacks, illegal traffic is in general unavoidable.

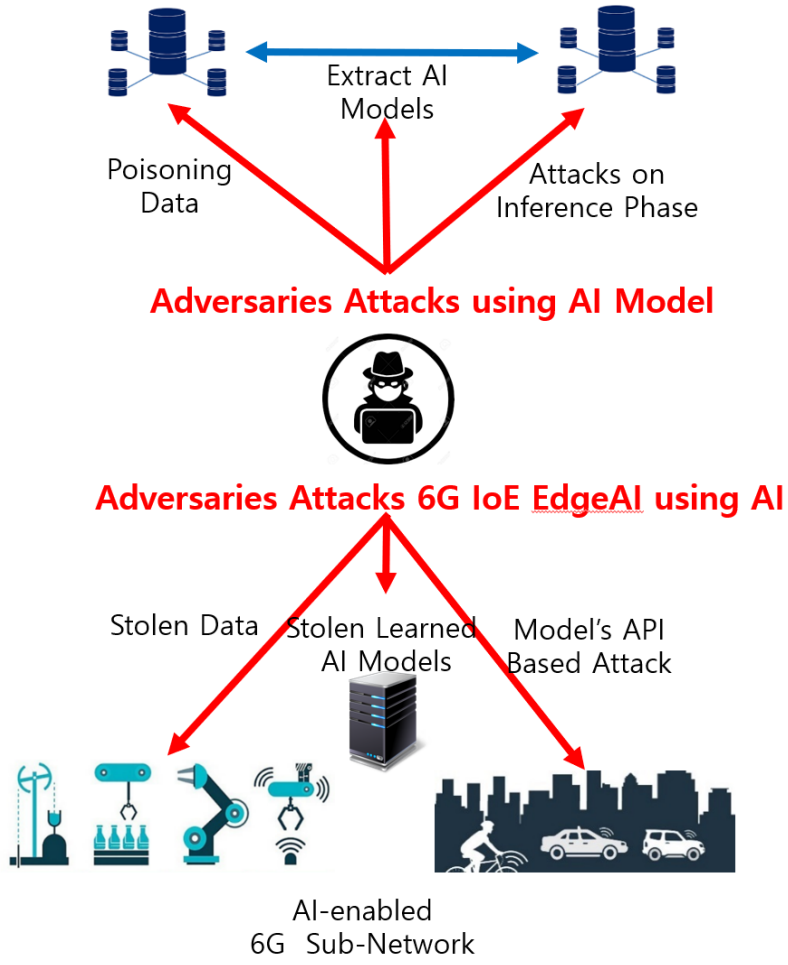

Figure 2. Structure of SDN, NFV, MEC Attack Detection Model

6G requires a massive amount of user data collected via billions of devices, and the users no longer foresee how external systems handle their data. For example, the 6G intelligent authentication systems depend on physical attributes and thus they may use private user data. Insecure IoT devices (ex: low powered sensors), which feed personal data to AI systems, are a major stepping stone for the attacker to launch attacks. Moreover, although edge-based federated learning preserves data privacy by imposing a physical control to maintain data closer to the user, the client ML/DL models being trained at the edge, could suffer from poisoning attacks launched from compromised IoT devices.

Compromised IoT devices feeding personal data to AI systems are a potential target for data theft. Model inversion attacks to retrieve the training data could also be a source for privacy violation. For known attacks against 6G privacy, fuzzing is basically used to identify each attack and collect the necessary data sets suitable for privacy learning. In particular, IoE EdgeAI-based federated learning preserves data privacy by imposing a physical control to maintain data closer to user. The data can be automatically labeled by the fuzzer. Once the datasets are generated, we can train DNN models to detect privacy attacks. In this way, we do not need to extract the features of such attacks. Through this, we could save a large amount of manual effort and increase the reliability and precision of the data we have obtained. The DNN models developed

through the proposed study will be verified by applying it to the AI enabled 6G smart factory sub-network and AI-enabled 6G transportation sub-network virtual environment built by the research team. Through experiments, we evaluate effectiveness of the trained DNN models in detecting the above-mentioned attacks. In addition, we will evaluate the models robustness against poisoning attacks and adversarial attacks.

4. CONCLUSIONS

In this paper, we raised security and privacy issues inherited from 5G networks to 6G networks and presented a model to solve them. In addition, a method for detecting abnormal traffic expected in 6G networks based on ML/DL and a method for implementing it were presented. Currently, our proposed method has been implemented at the prototype level. In addition, noteworthy results can be confirmed through continuous experimental studies.

Currently, we are conducting various experiments. In this process, the maximum attack detection rate is 99%. For the objectivity and accuracy of the experiment, additional analysis studies are underway. In the future, we plan to derive more specific algorithm implementation, experimental results, and prove the experimental results through various simulations.

ACKNOWLEDGEMENTS

This research was supported by the International Research and Development Program of the National Research Foundation of Korea(NRF) funded by the Ministry of Science and ICT(2022K1A3A1A79085890). This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2022-00207391, Development of Hashgraph-based Blockchain Enhancement Scheme and Implementation of Testbed for Autonomous Driving).

REFERENCES

[1] Chamitha De Alwis, Anshuman Kalla, Quoc-Viet Pham, Pardeep Kumar, Kapal Dev, Won-Joo Hwang, Madnusanka Liyanage, “Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research,” IEEE Open Journal of the communications Society, April 2021.

[2] Shunliang Zhang, “Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities.” Computer Networks, Volume 183, 2020.

[3] Yushan Siriwardhana, Pawani Porambagey, Madhusanka Liyanagez, Mika Ylianttila. “AI and 6G Security: Opportunities and Challenges,” Conference: 2021 Joint European Conference on Networks and Communications (EuCNC) & 6G Summit, 2021.

[4] W. Saad, M. Bennis, and M. Chen, “A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems,” IEEE Network, vol. 34, no. 3, pp. 134–142, 2019.

[5] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage et al., “6G White Paper: Research Challenges for Trust, Security and Privacy,” arXiv preprint arXiv:2004.11665, 2020.

[6] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, “Overview of 5G Security Challenges and Solutions,” IEEE Communications Standards Magazine, Vol. 2, No. 1, pp. 36–43, 2018.

[7] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, “A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions,” IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, pp. 196–248, 2019.

[8] P. Ranaweera, A. D. Jurcut, and M. Liyanage, “Survey on Multi-Access Edge Computing Security and Privacy,” IEEE Communications Surveys Tutorials, pp. 1–1, 2021.

[9] S. Wijethilaka, M. Liyanage, “Survey on network slicing for internet of things realization in 5g networks,” IEEE Communications Surveys & Tutorials, 2021.

[10] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8169–8181, 2019.

[11] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[12] Minghao Wang, Tianqing Zhu, Tao Zhang, J. Zhang, Shui Yu, Wanlei Zhou, "Security and privacy in 6G networks: New areas and new challenges," IEEE Communications Surveys & Tutorials, Vol. 21, No. 4. 2019.

[13] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Multi-layered Intrusion Detection and Prevention in the SDN/NFV enabled Cloud of 5G Networks using AI-based Defense Mechanisms," Computer Networks, vol. 179, p. 107364, 2020.

[14] R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine Learning Algorithms to detect DDoS Attacks in SDN," Concurrency and Computation: Practice and Experience, vol. 32, no. 16, p. e5402, 2020.

[15] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp.6822–6834, 2019.

[16] H. Fang, A. Qi, and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," IEEE Network, vol. 34, no. 3, pp. 24–29, 2020.

[17] H. Fang, X. Wang, and S. Tomasin, "Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks," IEEE Wireless Communications, vol. 26, no. 5, pp. 55–61, 2019.

[18] J. Wang, G. Joshi, "Cooperative SGD: A unified Framework for the Design and Analysis of Communication-Efficient SGD Algorithms, 2019.