AI and 6G Security: Opportunities and Challenges

Yushan Siriwardhana*, Pawani Porambage†, Madhusanka Liyanage‡, Mika Ylianttila§
*†‡§Centre for Wireless Communications, University of Oulu, Finland
‡School of Computer Science, University College Dublin, Ireland
Email: *†‡§[firstname.lastname]@oulu.fi, ‡madhusanka@ucd.ie

2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) | 978-1-6654-1526-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/EUCNC/6GSUMMIT51104.2021.9482503

***Abstract*—While 5G is well-known for network cloudification with micro-service based architecture, the next generation networks or the 6G era is closely coupled with intelligent network orchestration and management. Hence, the role of Artificial Intelligence (AI) is immense in the envisioned 6G paradigm. However, the alliance between 6G and AI may also be a double-edged sword in many cases as AI's applicability for protecting or infringing security and privacy. In particular, the end-to-end automation of future networks demands proactive threats discovery, application of mitigation intelligent techniques and making sure the achievement of self-sustaining networks in 6G. Therefore, to consolidate and solidify the role of AI in securing 6G networks, this article presents how AI can be leveraged in 6G security, possible challenges and solutions.**

***Index Terms*—6G, 6G Security, Artificial Intelligence, Machine Learning, Intelligent Security**

I. Introduction to 6G

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. Future networks must possess novel technologies that enable the digital virtual worlds with connected intelligence, to address the communication and networking challenges beyond 2030. While the conventional applications such as multimedia streaming will remain, literature envisions new application domains for 6G systems such as multisensory extended reality (XR) applications, Connected Robotics and Autonomous Systems (CRAS), and wireless Brain-Computer Interactions (BCI) [1]. Holographic telepresence, eHealth including in-body networks are a few other 6G use cases [2] that demand extremely high data rates, ultra-low latency and ultra-reliability.

The evolution of 6G application domains calls for an innovative network architecture beyond current network designs [3]. An open and distributed reference framework for 6G architectural building blocks defined by Nokia Bell Labs comprises four major interworking components [4]. These are platform, functional, specialized, and orchestration, covering the physical layer to the service layer with the following distinguishing features. The "het-cloud" is a heterogeneous cloud environment that eases the creation, placement and scaling of dynamic cloud services. 5G core network service-based architecture will extend to the Radio Access Network (RAN), named "RAN-core convergence". It will harmonize the RAN and core functions to create simpler networks [4]. Even smaller "sub-networks" such as in-body networks will emerge, which generally operate in a standalone fashion while benefiting from the wide area network.

6G will take the network softwarization/cloudification into network intelligentization, revolutionizing wireless networks from connected things to "connected intelligence" [1], [2]. Hence, AI becomes an integral part of the network, which plays a crucial role. The distributed heterogeneous networks require ubiquitous AI services to ensure the fulfilment of 6G goals. Intelligent wireless communications, closed-loop optimization of networks, big data analytics for 6G emphasize the use of AI in diverse aspects of 6G networks.

Beyond 2030 wireless applications will demand much higher data rates (up to 1 Tb/s), extremely low end-to-end latency (< 1 ms), extremely high end-to-end reliability (99.99999%) [1], [2]. 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 networks requires sophisticated security mechanisms. The security systems designed for 5G using the concepts of SDN and NFV should be further improved to cater to the security demands in 6G [5]. 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. This paper discusses the role of AI in the security provision of 6G networks.

The remainder of the paper is organized as follows: Section II outlines the security threat landscape in 6G. Section III discusses the role of AI in 6G security and privacy. Section IV highlights the issues and possible solutions. Finally, Section V concludes the paper.

II. Security Threat Landscape of 6G

This section presents the security issues of 6G networks. Pre-6G security explains the security issues inherited from 5G to 6G. The section also discusses security issues resulting from architectural changes and novel technologies used in 6G. Figure 1 illustrates possible attacks on different layers of the 6G architecture. Figure 2 depicts a summary of how this paper presents the security threat landscape of 6G.

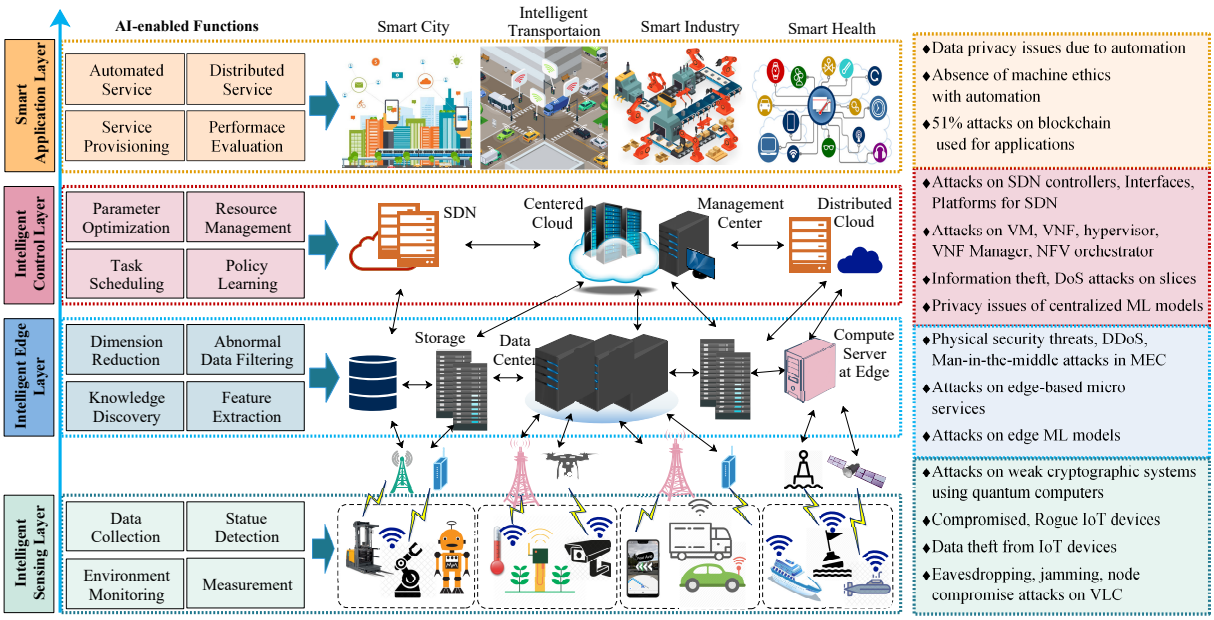

Fig. 1: Intelligent 6G Architecture [6], and 6G Security and Privacy Issues.

A. *Pre-6G Security*

Network softwarization technologies in 5G such as Software-Defined Networking (SDN), Network Function Virtualization (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 [7]. NFV related security issues are attacks targeting Virtual Machines (VM), Virtual Network Functions (VNF), hypervisor, VNF manager, NFV orchestrator[8]. Due to the massively distributed nature of 6G systems, MEC in 6G is subjected to physical security threats, Distributed Denial of Service (DDoS), man-in-the-middle attacks[9]. Potential attacks for network slicing are DoS attacks, information theft via compromised slices[10]. Attacks on network softwarization technologies fail the 6G network from achieving the promised dynamicity and full automation.

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 [11]. The resource-constrained IoT devices cannot afford complicated cryptography to maintain strong security [12], 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 local 5G network deployments usually provide services for verticals such as industries, healthcare, education. 6G further expands the concept by allowing even smaller networks like in-body networks, swarms of drones, environmental sensor networks with longer battery life [4]. These local networks operate as a standalone network and interwork with wide area connectivity when needed. In contrast to the well-defined local 5G networks, many stakeholders implement local 6G networks with different embedded security levels. A local 6G network with minimal security provides intruders with the opportunity to initiate attacks. And then infiltrate the networks which trust the compromised network.

B. *Security of 6G Architecture*

6G cells will shrink from small cells to “tiny cells” [1], and denser deployment of cells, mesh networks, multi-connectivity, and Device-to-Device (D2D) communications will be a norm. Malicious parties have a better potential to attack a distributed network with more vulnerable devices, each having mesh connectivity, thereby increasing the threat surface. The definition of sub-networks requires a change in the security strategy. Security provision for the massive number of devices within each sub-network by the wide area network is far from practical. A hierarchical security mechanism that distinguishes the sub-network level communication security and sub-network to wide area network security would be a better approach in 6G. The RAN-Core convergence makes higher layer RAN functions more centralized and coexist with the distributed core functions as User Plane Micro Services (UPMS) and Control Plane Micro Service (CPMS) [4], possibly at the edge. Attackers can target UPMS and CPMS, affecting multiple radio units served by micro-services. 6G networks will coexist with frameworks like Zero-touch net-

work and Service Management (ZSM) architecture [13] to enable short time-to-market of services, low operational cost, and reduced human error. Full automation equipped with self-learning causes the attacks to propagate in the closed-loops. Data privacy protection is challenging due to the vital need for automation with lesser human intervention in zero-touch networks. Implementing automated machine ethics is also an open question in fully automated 6G networks.

C. Security of 6G Technologies

6G rely on AI to enable fully autonomous networks. Therefore, attacks on AI systems, especially Machine Learning (ML) systems, will affect 6G. Poisoning attacks, data injection, data manipulation, logic corruption, model evasion, model inversion, model extraction, and membership inference attacks are potential security threats against ML systems [14]. 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. Blockchain is also a pivotal technology to unleash the potential of 6G systems. Blockchain is suitable for decentralized resource management, spectrum sharing, service management in massively large and distributed 6G networks [15]. 51% attacks are feasible with quantum computers to destabilize the blockchain. As the blockchain networks stores data publicly, privacy preservation is challenging. The current 5G standard does not concern the security issues due to quantum computing; rather, it depends on traditional cryptography like Elliptic Curve Cryptography (ECC) [5]. 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 [16]. Thus, the secure 5G communications enabled with asymmetric key cryptography may be no longer useful for post-quantum security without the design of quantum-safe cryptographic algorithms. Visible Light Communication (VLC) is also a technology suitable for indoor based systems such as positioning systems and outdoor systems such as vehicle-to-vehicle communication. Common attacks against VLC systems such as eavesdropping, jamming, node compromise systems [17] prevents the safe use of VLC.

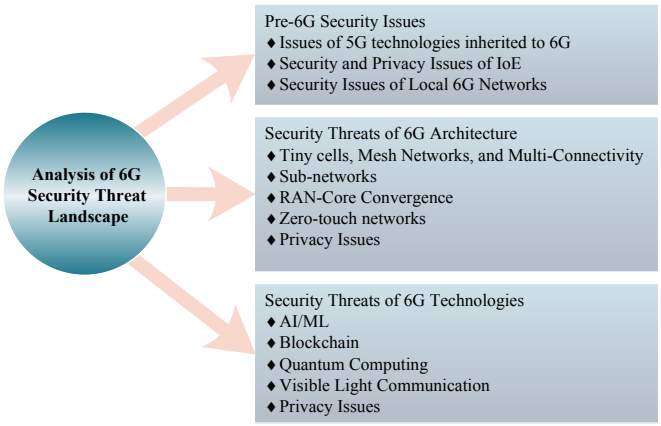

Fig. 2: Analysis of 6G Security Threat Landscape.

III. AI for Security and Privacy in 6G

Intelligent security and privacy provision is a part of AI's role in 6G systems. This section presents AI's use in pre-6G security, security of 6G architectures, security of 6G technologies, and AI for 6G privacy. Figure 3 illustrates AI's role as a defender for 6G applications.

A. Use of AI to Identify/Mitigate Pre-6G Security Issues

Multilayered intrusion detection and prevention using deep reinforcement learning and Deep Neural Networks (DNN) is viable in SDN/NFV-enabled networks [18]. They effectively defend against 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 [19]. ML-based adaptive security approaches are effective against attacks on SDN/NFV as the 6G networks expect dynamic placement of virtual functions on-demand. The attacks also evolve using AI techniques to learn vulnerabilities in a vastly distributed 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 generation make the conventional authentication/authorization systems insufficient for adequate security provision in large-scale IoT. Anomaly-based intrusion detection systems in Industrial IoT (IIoT) [20] detect malicious packets based on their behaviour. These learning-based detection systems utilize various features of the data as the input, therefore, suitable for detecting zero-day attacks. The use of communication link attributes and user behaviours with machine learning for authentication and authorization [21], [22] is a better approach in future networks for resource-constrained devices. In that way, devices do not utilize their limited resources to provide additional complex security.

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 from those sub-networks. Massive data transfer from one sub-networks to another might be of no use as these networks usually operate standalone. A sub-network can share only the learned security intelligence to another for communication efficiency [23]. A second sub-network can use the shared intelligence, feed it into its ML models, determine the malicious traffic of other networks, and apply dynamic policies.

B. Use of AI to Mitigate Security Issues of 6G Architecture

6G will primarily depend on edge intelligence compared to present centralized cloud-based AI systems. The distributed nature enables the execution of edge-based federated learning for network security in the massive device and data

regime [24], ensuring communication efficiency. 6G architecture envisages connected intelligence and uses AI at different levels in network hierarchy [6]. AI at the tiny cell level has the potential to block DoS attacks on cloud servers at the lowest level. The Multi-connectivity of a device in a mesh network allows several base stations to evaluate the behavior of a device using AI classification algorithms, and collectively decide the authenticity using weighted average schemes as in [25]. The behaviour based approaches reduce the overhead caused by frequent key exchanges as the tiny cells and multiple access technologies cause frequent handovers. Different levels of authorization are possible for sub-network level and wide area network level with federated learning. The trust score learned within the sub-network level can be shared outside only when external communication is needed. Learning based intrusion detection approaches [18], [19] can be good candidates to prevent attacks on CPMS and UPMS as the edge already possess the data for intelligent service provision. Frameworks like ZSM are equipped with domain analytics and domain intelligence services for zero-touch management of networks, predominantly based on AI. AI model assessment, AI engine for API security are key security functional components that enhance the security of ZSM reference architecture [26].

C. Use of AI to Mitigate Security Issues of 6G Technologies

The predictive analytics using AI can predict attacks such as 51% attacks on blockchain before the attack occurs. A quantum computer may threaten asymmetric key cryptography. However, they can provide exponential speed-ups for AI/ML algorithms to perform tasks much faster and realize previously impossible tasks. Hence, quantum machine learning for network security is a potential defence technique against quantum computer based attacks [27]. Intelligent beamforming techniques based on Reinforcement Learning (RL) provide optimal beamforming policy against the eavesdropper attacks in VLC systems [28]. Jamming resembles DoS attacks; therefore, anomaly-based detection systems equipped with AI is a possible solution to detect jamming attacks. AI-based authentication and authorization systems are also suitable for preventing node compromise attacks [21].

D. Use of AI for 6G Privacy

Multi-connectivity, mesh networks with tiny cells in 6G allow simultaneous communication for devices via multiple base stations. 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 [23] keeps data in the user's proximity compared to cloud-based centralized learning to enhance data privacy and location privacy. The 6G sub-network level AI allows privacy preservation within the sub-network 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 intelligent models, users would prefer different privacy levels on different applications. AI-based service-oriented privacy-preserving policy updates [29] is a potential solution to support fully automated 6G networks with preserved privacy.

IV. Issues and Counter-measures

Despite the importance of AI in 6G systems, AI has its security, privacy, and ethical issues. Moreover, AI can be an instrument to launch intelligent attacks. This section presents the privacy, security, ethical issues in AI and potential solutions to overcome them. Figure 3 also illustrates AI's role as a defender for 6G applications.

A. Security Issues in AI

1) Issues: 6G achieves connected intelligence via AI-enabled functions, especially with ML systems that are subjected to security threats. Poisoning attacks influence the learning phase of a ML system, which lead the model to learn inaccurately. For example, data injection, data manipulation, and logic corruption are some of the poisoning attacks. Evasion attacks try to avoid the model during the inference phase using carefully crafted adversarial examples. Model extraction, model inversion, and membership inference are API based attacks on ML models [14].

2) Solutions: Potential countermeasures such as adversarial machine learning and moving target defence can create resilient AI systems. Input validation and robust learning against poisoning attacks, adversarial training and defensive distillation against evasion attacks, and differential privacy and homomorphic encryption against API based attacks are other defence mechanisms. The balance between the increased defence and performance degradation is a design challenge with these defence mechanisms [14].

B. Privacy Issues in AI

1) Issues: Due to AI's ability of large scale data analysis combined with the speed of future computers and automation needs of future networks, AI can easily compromise privacy. 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 proposed intelligent authentication systems depend on physical attributes [22], may use private user data. Insecure IoT devices (ex: low powered sensors) feeding personal data to AI systems, are a potential target for data theft. Model inversion attacks on ML to retrieve the training data could also be a source for privacy violation [30].

2) Solutions: Edge-based federated learning preserves data privacy by imposing a physical control to maintain data closer to the user [30]. Homomorphic encryption, which allows performing mathematical operations without decrypting data, imposes a technical control for privacy preservation [31]. Further research on homomorphic encryption is needed to ensure learning with encrypted data produces the same output as with plain data. Differential privacy techniques can add random noise to the training data and prevent private information disclosure towards learning models [32].

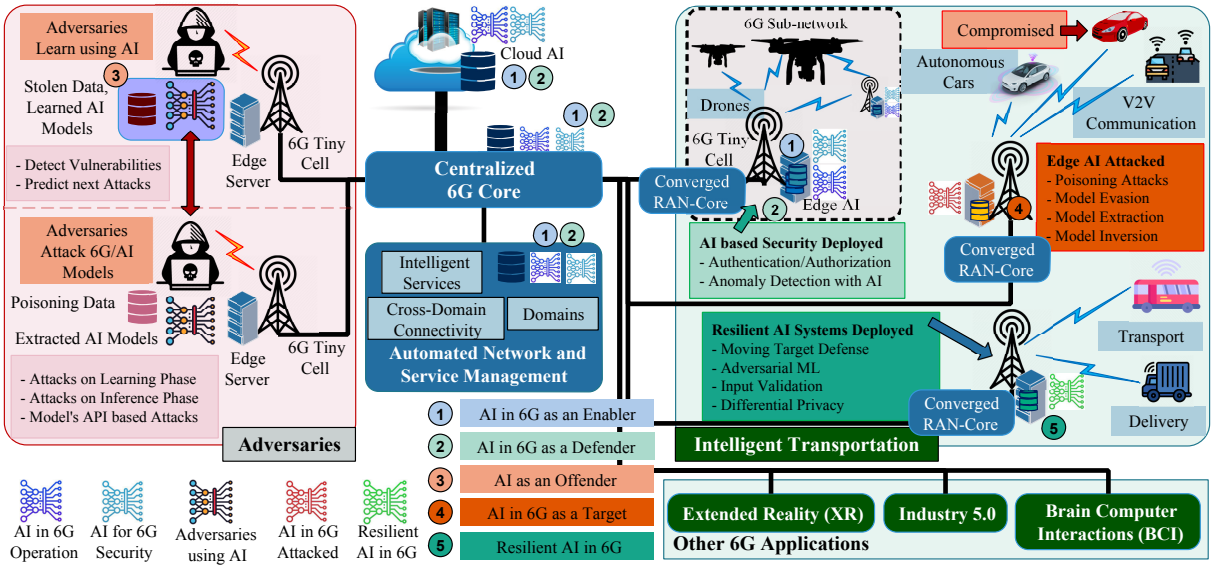

Fig. 3: AI's role as an Enabler, Defender, Offender and a Target in 6G Intelligent Transportation.

C. Ethical Issues in AI

1) Issues: Fully automated AI-based 6G networks need lesser human interventions in network operations. The way machines learn differs from how humans perceive things, and machines do not address ethical considerations as humans. AI systems behave according to the way they were taught and trained. However, they are not capable of behaving against the logic in exceptional situations as done by humans.

2) Solutions: "Ethics by Design" [33] approach brings the debate on ethical implications at the primary stage of the design of AI systems. Considering ethics at the early stage could be useful in intelligent 6G systems. Guidelines, laws, and regulations [34] are possible measures to address data ethics and ownership in the context of 6G to achieve a proper balance between risk and benefit [6]. Automated machine ethics needs to be defined to ensure data privacy in future networks.

D. Use of AI for Attacking 6G

1) Issue: With the ability to make network-wide intelligent decisions with distributed edge-based architecture, AI itself can uncover the patterns within a large volume of data at different levels (intelligent radio, edge, and cloud). Hence, AI-based mechanisms have the potential to uncover vulnerabilities of the network. For example, AI can learn the most vulnerable IoT devices, convert them into bots and initiate DDoS attacks [14] against a critical node.

2) Solution: The countermeasure for AI based intelligent attacks is also the implementation of more intelligent defence systems. They can be empowered by AI itself using distributed intelligence. Moving target defence techniques is a proactive measure that introduces dynamicity to the network [35], and weakens the learning process of AI-enabled attackers. Quantum machine learning could also be used to design advanced defence techniques to resist AI-based attacks [27].

TABLE I: Significance/Importance of AI based Security/Privacy Solutions and Attacks on different 6G Applications

	AI based Security/Privacy Solutions								Attacks on AI/ML					
Potential 6G Applications	**Anomaly based Intrusion Detection**	**Machine Learning for Authentication and Authorization**	**Quantum ML**	**Service oriented Privacy using AI**	**Adversarial ML**	**Differential Privacy**	**Homomorphic Encryption with ML**	**Blockchain with AI**	**Dataset Poisoning**	**Algorithm Poisoning**	**Model Poisoning**	**Model Evasion**	**Model Inversion**	**Model Extraction**
Multisensory Extended Reality (XR)	H	M	M	H	M	M	L	M	H	M	H	H	M	M
Connected Robotics and Autonomous Systems (CRAS)	H	H	H	H	H	M	M	H	H	H	H	H	H	M
Wireless Brain-Computer Interactions (BCI)	M	M	L	L	M	H	H	L	H	M	H	H	H	H
Smart Grid 2.0	H	M	H	L	M	L	L	H	H	H	H	H	H	M
Industry 5.0	H	H	M	M	H	M	M	M	H	M	H	H	H	M

Low Importance Medium Importance High Importance

V. Conclusions

AI is a key enabler for the next generation 6G mobile networks and ensuring security is a critical consideration to realize 6G vision. AI-enabled 6G security provides intelligent, robust security solutions. This paper provides an overview to comprehend the multitude of opportunities and challenges of having intelligent security and privacy provision as a part of AI's role in 6G systems. Moreover, it also identifies future research directions by discussing challenges in AI-based security and privacy provision and suggest viable solutions.

Acknowledgement

This work is supported by Academy of Finland in 6Genesis Flagship (grant no. 318927) and 5GEAR (Grant No. 319669) projects. The research leading to these results partly received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

References

[1] 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.

[2] C. de Alwis, A. Kalla, Q. V. Pham, P. Kumar, K. Dev, W. J. Hwang, and M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2021.

[3] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[4] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen, and K. Hätönen, "6G Architecture to Connect the Worlds," *IEEE Access*, vol. 8, pp. 173 508–173 520, 2020.

[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] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[7] 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.

[8] R. Khan, P. Kumar, D. N. K. Jayakody, and 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.

[9] 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.

[10] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, 2021.

[11] 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.

[12] 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.

[13] ETSI, "Zero-touch Network and Service Management (ZSM)," ETSI GS ZSM 002 - Reference Architecture, Aug 2019.

[14] C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" *IEEE Network*, vol. 34, no. 6, pp. 140–147, 2020.

[15] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[16] A. Dogra, R. K. Jha, and S. Jain, "A Survey on beyond 5G Network with the Advent of 6G: Architecture and Emerging Technologies," *IEEE Access*, 2020.

[17] G. Blinowski, "Security of Visible Light Communication Systems — A Survey," *Physical Communication*, vol. 34, pp. 246–260, 2019.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] C. Ma, J. Li, M. Ding, H. H. Yang, F. Shu, T. Q. S. Quek, and H. V. Poor, "On Safeguarding Privacy and Security in the Framework of Federated Learning," *IEEE Network*, vol. 34, no. 4, pp. 242–248, 2020.

[25] Z. Chkirbene, A. Erbad, R. Hamila, A. Gouissem, A. Mohamed, M. Guizani, and M. Hamdi, "Weighted Trustworthiness for ML based Attacks Classification," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2020, pp. 1–7.

[26] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 2020.

[27] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum Machine Learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[28] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep Reinforcement Learning-enabled Secure Visible Light communication against Eavesdropping," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 6994–7005, 2019.

[29] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G Privacy: Scenarios and Solutions," in *2018 IEEE 5G World Forum (5GWF)*, 2018, pp. 197–203.

[30] 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.

[31] J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy Preservation for Machine Learning Training and Classification based on Homomorphic Encryption Schemes," *Information Sciences*, vol. 526, pp. 166–179, 2020.

[32] T. Zhang, T. Zhu, P. Xiong, H. Huo, Z. Tari, and W. Zhou, "Correlated Differential Privacy: Feature Selection in Machine Learning," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2115–2124, 2020.

[33] M. d'Aquin, P. Troullinou, N. E. O'Connor, A. Cullen, G. Faller, and L. Holden, "Towards an 'Ethics by Design' Methodology for AI Research Projects," in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018, pp. 54–59.

[34] E. Bird, J. Fox-Skelly, N. Jenner, R. Larbey, E. Weitkamp and A. Winfield, "The Ethics of Artificial Intelligence: Issues and Initiatives," European Parliamentary Research Service, March 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

[35] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 709–745, 2020.