Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(Research Article)

A taxonomical survey of 5G and 6G security and privacy issues

Jairus Ekume Ounza *

Department of ICT, Kabarak University, Kenya.

Global Journal of Engineering and Technology Advances, 2023, 14(03), 042–060

Publication history: Received on 31 January 2023; revised on 10 March 2023; accepted on 12 March 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.14.3.0047

Abstract

Extensive research has been done on 5G and 6G security challenges. It has been shown that these challenges have the potential of affecting cross board 5G and 6G ecosystems such as technologies, services and applications. The perspective of the currently identified security challenges vary depending on the researcher's area of concern. This survey generated a consolidated source of information on the taxonomy of 5G and 6G ecosystem security challenges necessary for addressing both pre and post security issues to be encountered upon 5G and 6G implementation.

Keywords: Attacks; Privacy; Security; 5G; 6G; Networks

1. Introduction

Wireless technology has been widely adopted due to its ability to transcend terrestrial obstacles. This technology has advanced tremendously since the first generation to the current yet to be deployed 6G. 5G, which is a predecessor of 6G provide higher capacities, higher data rates, lower latency, massive device connectivity, lower cost, and better consistent quality of service than 4G networks [1]. 5G networks are expected to deliver extensive variety of services comprising enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (uRLLC), and massive type of communications (mMTC) [2]. The emergence of the internet of things (IoT) has led to the need for higher rates in the wireless networks evolution. Although 5G has proved an evolutionary generation for connecting, supporting IoT networks and providing new services, as well as offering significant improvement over the existing systems, it will not be able to fulfill the demands of future emerging intelligent and automation systems [3]. The unprecedented growth of new IoT services is on-going to consider a broad range of applications, such as extended reality (XR) services, telemedicine, haptics, drones, brain computer interfaces, and connected autonomous systems [4]. The 6G on its part will be driven by emerging technologies, services and applications. Networking and communication scientific community envisage that 6G will be driven entirely by network orchestration and management [5], [6], [7]. 6G will be characterized by the following factors [8]:

- AI integrated communication
- Tactile Internet
- High energy efficiency
- Low backhaul and access network congestion
- Enhanced data security
- As concerns related to the migration implementation of 6G are being addressed [9], there is also need to consider emerging vulnerabilities and threats that may affect 6G security [9].

The contributions of this paper include the following:

- A 5G brief review and a summary background on 6G technologies, services and applications are provided.

*Corresponding author: Jairus Ekume Ounza

- A summary of security issues across 6G ecosystem (technologies, services and applications) is given.
- A summary of solutions for 6G ecosystem (technologies, services and applications) security issues is provided.

The rest of this paper is structured as follows: Section 2 discusses 5G and 6G networks in general, while Section 3 presents the various 6G ecosystem technologies. On the other hand, Section 4 discusses the general 6G services, while Section 5 presents specific 6G applications. Similarly, Section 6 discusses the general wireless technology security pathway, while Section 7 presents the 6G Security threats and vulnerabilities. On the other hand, Section 8 discuses the various solutions to 6G threats and vulnerabilities. Finally, Section 9 concludes the paper and offers some future research work. Table 1 presents the acronyms used throughout this paper.

Table 1 Acronyms

5G	Fifth Generation
6G	Sixth Generation
eMBB	Enhanced mobile Broadband
uRLLC	Ultra-Reliable and Low-Latency communication
mMTC	Massive Machine-Type Communication
IoT	Internet of Things
XR	Extended reality
AI	Artificial Intelligence
THz	Sub-Terahertz
UAV	Unmanned aerial vehicles
3 D	Three-Dimensional
MIMO	Multiple-Input Multiple -Output
FSO	Free space Optical
MBRLLC	Mobile broadband reliable low-latency communication
mURLLC	Massive URLLC
HCS	Human-centric services
MPS	Multi-protocol SerDes
3CLS	Convergence of communication, control, localization and sensing
WET	Wireless Energy Transfer
AR	Augmented Reality
VR	Virtual Reality
MR	Mixed Reality
CAV	Connected autonomous vehicles
QoL	Quality of Life
IWD	Intelligent wearable devices
IIoMT	Intelligent Internet of Medical of Things
H2H	Hospital-to-Home
DLT	Distributed ledger technology
NFV	Network function virtualization
SDN	Software defined networking

API	Application programming interfaces
DoS	Denial of service
DDoS	Distributed Denial of Service
AI/ML	Artificial Intelligence/Machine Language
E2eE	End to End
SLA	Service level agreement
VM	Virtual machine
VLC	Visible Light Communication
VPN	Virtual private networks
IPsec	Internet Protocol Security

2. The 5G and 6G Networks

An increase in wireless data traffic volume and magnitude of connected things is expected to leap to hundredfold of equipment in a given cubic meter. Data hungry applications such as sending holographic videos require a spectrum bandwidth that is currently unavailable in the mm-wave spectrum. This is a challenge on an area of spatial spectral efficiency and the needed frequency spectrum bands for connectivity hence a need for a broader radio frequency spectrum bands for connectivity. It is expected that this will be addressed by broader radio frequency spectrum bandwidth which can only be found at the sub-terahertz (THz) and THz bands [10]. The recent upsurge of diversified mobile applications, especially those supported by Artificial intelligence (AI) technology is spurring heated discussions on the future evolution of the wireless communication [11], [12]. 5G applications are considered under three services, eMBB, URLLC, mMTC [13] as shown in Table 2 below.

Table 2 5G service types

Research	Service type	Focus Area
[13]	Enhanced mobile Broadband (eMBB)	eMBB applications prioritizes prioritize high throughput, capacity and spectral efficiency
	Ultra-Reliable and Low-Latency communication (URLLC)	High reliability low latency
	Machine- Type Communication mMTC	Energy efficiency an massive connectivity

3. 6G Ecosystem Technologies

6G can be framed into one big vision statement of ubiquitous wireless intelligence. It will experience unparalleled revolution that will re-shape the wireless evolution from `` connected things” to “connected intelligence.” 6G will support ubiquitous services from core to the end devices of the network. AI will be the driving force in designing and optimizing 6G architectures, protocols and operations [14],[15]. Although AI has not been used in the previous generations of mobile technologies it will be essential in the development of 6G in order to automate resources management [16] and improve air interface algorithms [17]. 6G will satisfy future expectations of IoT applications and overcome the restrictions of 5G networks [18], [19]. 6G will be able to ```connect everything, provide full dimensional wireless coverage, integrate all functions, including sensing, communication, computing, caching, control, positioning, radar, navigation, and imaging to support full-vertical applications’’[20].Major technology trends promoting the development of 6Ginclude; terahertz: essential to implement mobile networks that can be integrated with sensing to provide optimized transport management, a need for three-dimensional vertical networks to integrate satellite and cellular communication to support seamless connections of (UAV’s), artificial intelligence to enhance network performance and decrease the computational complexity of network operation, green and sustainable design a critical requirement of mobile networks which promotes development of 6G [21].Table 3 below represents some of technologies identified by previous researchers that will that are being considered for 6G.

Table 3 6G technologies

Authors	**Research contributions**	**Focus Area**
		Technologies
[22]-[25]	Discusses the emergence of the optical wireless technology along radio frequency and its support to upcoming 6G applications	Optical wireless communication systems
[26] [28]-[31]	Focuses on how the bandwidth [27] can be increased so that it's able to support the upcoming 6G technology.	Terahertz Band
[32] [33] [35] [36] [37]	Brings to attention the importance of AI [34] and its role as a key enabler towards the roll out of emerging 6G technologies	Artificial Intelligence
[38] [39]	Discusses about integration of ground and airborne networks to users in the vertical extension.	3D Networking
[40]	Explains on the importance of unsupervised learning which will play a key role against cyber attacks [41]	Quantum communication
[42] [43]	Contributes to how mMIMO technique can be used to improve spectral efficiency	Massive MIMO
[44]	Duels on how devices without batteries will be supported in 6G connections. It also focuses on lengthening the lifetime of the battery charging wireless systems.	Integration of wireless information and energy transfer
[45]	Discusses on how to handle and manage big data.	Big data analytics
[46] [47] [49]-[52]	Discusses on management of massive data [48] through distributed ledger technology	Block chain
[53] [54]	Enlightens on big data computing	Mobile edge computing
Author(s)	**Research contributions**	**Focus area**
		Medium of communication
[55] [57] [58]	Focuses on how to integrate terrestrial and non-terrestrial networks to extend wireless [56] coverage.	Integrated space terrestrial network
[8]	Identifies the limitations of optical fibre links and the strengths of the FSO front haul/backhaul. The limitation areas of usage and the application of FSO front haul/backhaul are also explained.	FSO front haul/backhaul network
[59]	Discusses about the benefits of having UAV's as compared to fixed base stations	Unmanned aerial vehicles/Drones

4. 6G Services

5G Compatible application will be central to the emerging 6G on a broader scale. Several emerging fast paced solutions are expected to be deployed with 6G technologies.6G services will redefine those from the 5G by morphing the classic URLLC, eMBB with new services in the Table 4 below [60].

Table 4 6G services

Author(s)	**Service type**	**Performance indicators**
[4]	MBRLLC	-Stringent rate-reliability-latency requirements -Energy efficiency -Rate-reliability-latency in mobile environment
	mURLLC	-Ultra high reliability -Massive connectivity -Massive reliability Scalable URLLC
	HCS (Human-centric services)	-QOPE capturing wireless metrics as well as human and physical factors
	MPS	-Control stability Computing latency -Localization accuracy -Sensing and mapping accuracy. -Latency and reliability for communications -energy
	Multipurpose 3CLS.	-Deliver 3CL services -Provide wireless energy transfer (WET) to smart devices.
[60]	Network Slicing	-Supports a range of service requirements

5. 6G Applications

The emergence of new applications that will define 6G is taking shape. These applications will drastically shape the human society of 2030's and beyond. The general performance expectations and security requirements will become more complicated with the emergence of very capable ubiquitous threat matrix [9].Different author have addressed a number of these emerging applications. Some other applications cut across their literature while others are individualized. These applications have been summarized in Table 5 below to give an overview of how 6G will be useful.

Table 5 6G Applications

Author(s)	**Application**	**Purpose**
[61] [62]	UAV Based mobility (UAV)	UAV'S [63] will be used in new cases such a s passenger taxi, automated logistics and military operations.
[64] [65]	Holographic tele-presence	Will project realistic three dimensional (3D) images of distant people and objects with a high level of realism rivalling physical presence.
[66] [67]	Extended reality	Extended reality (XR) is a term used to refer all real and virtual combined environments which cover

		Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR and everything in between.
[68] [69]	Connected autonomous vehicles (CAV)	Will support vehicle requirements e.g. driver-less taxi and driver-less public transport
[70]	Smart Grid 2.0	Smart Grid 2.0 will offer features such as automated meter data analysis, distribution grid [71] management automation and reliable electric power delivery with self-healing capabilities
[72]	Industry 5.0	This industrial revolution will enable people to work alongside robots and smart machines to add a personal touch to the industry
[73] [74]	Intelligent health care	In a few years, AI –driven intelligent healthcare will be developed based on various new methodologies including Quality of Life (QoL), Intelligent wearable devices (IWD), Intelligent Internet of Medical of Things (IIoMT), Hospital-to-Home (H2H services and novel business models.
[75] [76]	Digital Twin	This is a novel industrial control and automation systems concept. A digital twin is defined as a digital or virtual copy of a physical object, an asset or a product.
[77]	Distributed ledger technology (DLT)	Block chain provide the advantage of disintermediation, immutability, non-repudiation, proof of governance, integrity and pseudonymity [78] are important to enable different services in a trusted and secure manner.
[79] [80]	Haptic communication	Enables expression through a sense of touch
[81]	Multi-dimensional reality	Enable 3D games or multi-dimensional video that interact with all five sense organs of the body to create an illusion of real-world by combining VR and AR to render a true gaming experience
[82] [83]	Tactile internet	Enables transmission of touch, feelings (sense) along with audio and video or other forms of responses.
[84] [86]	Wireless brain computer	Wireless [85] brain computer is expected to introduce new use-cases that need 6G connectivity. The imminent use-cases are expected to enable brain-controlled movie input to fully –fledged multi brain-controlled cinema

6. Wireless technology security pathway

Security in wireless technology is an evolving target. Early technologies (1G, 2G, 3G) encountered security challenges that included cloning, illegal physical attacks, eavesdropping, encryption issues, authentication, authorization problems, and privacy issues [87]. 4G networks were defined by security challenges that included MEDIA access control (MAC) layer security threats (denial of service attacks, eavesdropping, replay attacks), and malware applications (viruses, hardware tampering) [34]. 5G Security and privacy threats target access, backhaul, and core networks [9].They include cyber ware and critical infrastructure threats, Network function virtualization (NFV), software-defined networking (SDN), related threats and cloud computing related threats [88]. Some of the security threats due to SDN are critical due to the exposure of Application programming interfaces (API's) to unintended software, inception of Open Flow, centralized network control as a result of DOS attacks [89]. Although there are many 6G vision papers, only a handful of surveys have been released with key focus on 6G security and privacy issues. Table 6 summarizes some of the security issues in 5G networks.

Table 6 5G security threats and vulnerabilities

	Software-Defined Networking (SDN)
Author(s)	**Threat/Vulnerability**
[90]	Attacks on SDN controller
	Attacks on northbound and southbound interfaces
	Inherent vulnerabilities [91] of platforms used to deploy SDN controllers/applications
	Network Function Virtualization (NFV)
Research	Threat/Vulnerability
[92]	Attacks targeting virtual machines (VM)
	Virtual network functions (VNF), hypervisor, VNF manager, NFV Orchestrator
	Multi-Access Edge Computing (MEC)
[93]	Physical security threats
	Distributed Denial of Service (DDoS)
	Man- in the middle attack

7. 6G Security threats and vulnerabilities

The implementation of the above technologies vary with some being an advancement of the preceding technology 5G while others are specifically under development to be used once the implementation of 6G takes place. Security is key for the success of any technology including 6G. Some of the security threats and vulnerabilities are inherent due to the previous technologies while others will be exploits of the new technology 6G due to technological limitations, flaws and shortcomings. These security issues affect all the pillars of 6G technology that include technology, applications and services. This work summarizes these security vulnerabilities and threats to the 6G technology as in the Table 7 below.

Table 7 6G security threats and vulnerabilities

	Block Chain	
Author(s)	**Threat/Vulnerability**	**Impact**
[94] [95]	Double spending attack	User spending a single token multiple times
[96]	Re-entrance attacks	Occurs when a smart contract invokes another smart contract iterative
[97]	Sybil attacks	Attacker or a group of attackers try to hijack [98] the block chain peer network by conceiving fake identities
[99]-[102]	Privacy leakages	Leakage of transaction data privacy Leakage of smart contract logic privacy Leakage of user contracts

		Leakage of user privacy Privacy leakage while execution of smart contracts Revealing of information to competitors
	Quantum computing	
Author(s)	**Threat/Vulnerability**	**Impact**
[37]	Challenge of having device independent post quantum cryptography	Difficulty in providing solutions to prevent quantum based attacks
	Artificial intelligence/ Machine learning	
Author(s)	**Threat/Vulnerability**	**Impact**
[103]	Training phase poisoning attacks	The attacker can tamper the training data by injecting carefully crafted malicious [104] sample to influence the outcome of the learning method.
[105] [106]	Test phase evasion attacks	Attempts to circumvent the learned model by introducing disorders to the test data.
[37]	Comprise of AI frameworks	Exploits vulnerabilities artefacts or traditional attack vectors towards software, firmware and hardware elements
[37]	AI/ML API based attacks	An adversary queries and attack an API of a ML model to obtain predictions on input feature vectors which may lead to model inversion (Training data recovery), model extraction (model architecture comprising model confidentiality revelation) and membership inference (exploit model output to predict on training data and ML model) attacks.
	Terahertz technology	
Author(s)	**Threat/Vulnerability**	**Impact**
[37]	eavesdropping, and access control attacks	Exposes transmitted data transmitted to threats and vulnerabilities.
	Optical wireless communication (visible light communication technology)	
Author(s)	**Threat/Vulnerability**	**Impact**
[107]	Prone to eavesdropping attacks	Comprises confidentiality
	Open API's Security threats	
Author(s)	**Threat/Vulnerability**	**Impact**
[108] [109] [111]	Parameter attacks	Improperly validated [110] parameters may lead to injection attacks on cross-domain data services -Data injection, data manipulation and logic corruption -manipulating network topology data to insert fake links, malicious nodes. -Continuous injection of false parameters may lead DoS attack to make data services unresponsive

	Identity attacks	-Exploit laws in authentication and authorization -Extraction of API keys and using them as credentials -Attack insecure E2eE domain orchestration service to change configurations to fail SLA's, create new instances demanding more resources to exhaust the network
	Man-in the middle attack	-obtain information from unencrypted transmission of API messages between the API consumer and provider. -Interception of API messages and revealing confidential information
	Dos/DDoS attacks	-Make an API out of order by submerging it with massive amount of requests.
	Closed loop Automation	
Author(s)	**Threat/Vulnerability**	**Impact**
[108] [109] [111] [112]	Dos attacks	Fake heavy load on VNFs to increase the capacity of VM, which may lead to DoS
	Man-in-the-middle attacks	-Triggering a fake event and intercept the domain control messages to reroute traffic via a malicious switch
	Deception on attacks	Intends to tamper transmitted data
	Intent-Based Interfaces	
[108], [113]-[115]	Information Exposure	Intercepting information of intents by an unauthorized entities to compromise system security objectives(e.g. ., privacy, confidentiality [116] .This may lead to the launch of other attacks
	Undesirable configuration	Changing the mapping from intent to action. Setting the security level from ``High'' to``Low''
	Abnormal behaviours	Malformed intent could change the behaviour, causing network outage
	Mal-informed intent	Changing the intent reduce the service quality

8. Solutions to 6G threats and vulnerabilities

There exist solutions that have been outlined that will address threats and vulnerabilities prone to 6G. A summary of these solutions is outlined in Table 8 below.

Table 8 Solutions to 6G threats and vulnerabilities

Blockchain		
Author(s)	**Publication Year**	**Solution**
[117] [118]	2017 2018	Proper validation of correct functionality of smart contracts by identifying semantic flaws
[119] [120] [121]	2018 2018 2018	Using security check tools
[122] [123]		Pre-forming formal verification [124]
[37]		Proper access control

[125] [126] [127] [128]	2010 2009 2019 2018	Privacy by design and TEE
[129]	2021	Selecting proper block chain/DLT
	Quantum computing	
Author(s)	**Publication Year**	**Solution**
[130]	2020	Post quantum cryptographic primitives (Lattice-based, hash-based and multivariate-based cryptography
	Artificial intelligence/machine learning	
Author(s)	**Publication Year**	**Solution**
[131]	2017	Adversarial training injects perturbed examples similar to attacks [132] into training data to increase robustness
[133]	2019	Defensive distillation
[134]	2020	Against poisoning attacks in the training phase block chain provides a distributed, transparent and secure data sharing framework perspective
[135] [136]	2019 2019	Moving target defence
[137]	2020	Input validation [138]
[37]		Control of information provided by ML API's to the algorithm to prevent them
[139]	2018	Addition of noise to ML prediction
	Terahertz technology	
Author(s)	**Publication Year**	**Solution**
[140]	2019	Channel characterization of the backscatter
[141]	2017	-Sharing data transmission over multiple paths -Secure key exchange
[142]	2020	performing authentication at the physical layer in vivo nano-networks at THz frequencies
	Optical wireless communication **(visible light communication technology)**	
Author(s)	**Publication Year**	**Solution**
[143]	2019	Using linear precoding to enhance the performance of multiple-input multiple output (MIMO) VLC system.
[144]	2020	Exploitation of PLS
	Open API's Security threats	
	Parameter attacks	
Author(s)	**Publication Year**	**Solution**

[108] [109] [111]	2020, 2020 2021	-Input validation and user authentication. -Access control and rate limiting
	Identity attacks	
Author(s)	**Publication Year**	**Solution**
[108] [109] [111]	2020, 2020 2021	-Authentication (Signed JWT tokens, OpenID connect) -Authorization(Role based Access control, Attribute based access control list
	Man-in the middle attack	
Author(s)	**Publication Year**	**Solution**
[108] [109] [111]	2020, 2020 2021	-Use secure encrypted communication -Use of VPNs (e.g. IPsec, SSL/TLS and HIP
	Dos/DDoS attacks	
Author(s)	**Publication Year**	**Solution**
[108] [109] [111]	2020 2020 2021	-Throttling/rate limiting the usage of APIs -Deployment of API gateways and micro gateways -AI based API security for proactive monitoring
	Closed loop Automation	
	Dos attacks	
Author(s)	**Publication Year**	**Solution**
[108] [109] [111] [112]	2020 2020 2021 2020	-Throttling /rate limiting on resources for VMS -AI based resources level prediction
	Man-in-the-middle attacks	
Author(s)	**Publication Year**	**Solution**
[108] [109] [111] [112]	2020 2020 2021 2020	-Use secure encrypted communication -Use of VPN's(e.g. IPsec, SSL/TLS and HIP
	Deception on attacks	
Author(s)	**Publication Year**	**Solution**
[108] [109] [111] [112]	2020 2020 2021 2020	- Use Integrity validation mechanisms (e.g. Block chain)
	Intent-Based Interfaces	
	Information Exposure	

Author(s)	Publication Year	Solution
[108] [113] [114] [115]	2020 2020 2016 2020	-Authentication between intent producer and consumer (Signed JWT tokens, OpenID connect) -Controlled access via authorization controls (Role based Access Control, OAuth 2.0) -Secure communication via transport protocols (TLS 1.2)
	Undesirable configuration	
Author(s)	**Publication Year**	**Solution**
[108] [113] [114] [115]	2020 2020 2016 2020	-Input validation via user authentication
	Abnormal behaviours	
Author(s)	**Publication Year**	**Solution**
[108] [113] [114] [115]	2020, 2020 2016 2020	-AI Based proactive for abnormality detection
	Mal-informed intent	
Author(s)	**Publication Year**	**Solution**
[108] [113] [114] [115]	2020 2020 2016 2020	Intent format validation

9. Conclusion

This paper has provided an overview of consolidated current existing information related to 6G and 5G networks. Due to massive number of devices that will rely on network connectivity and the need towards using advanced technology in solving problems, this paper provides a useful source of reference. All key aspects that include technology, services, applications security in 5G and 6G proposed solutions have been considered. Since 6G is a technology yet to be rolled out, further studies should be focused towards specific areas of the technology because of 6G complexity and massive ecosystem.

Compliance with ethical standards

Acknowledgments

I would like to appreciate the members of the ICT department for the assistance offered during the drafting and writing of this manuscript.

References

[1] Gupta A, Jha RK. A survey of 5G network: Architecture and emerging technologies. IEEE access. 2015 Jul 28;3:1206-32.

[2] Alsharif MH, Kelechi AH, Albreem MA, Chaudhry SA, Zia MS, Kim S. Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions. Symmetry. 2020 Apr 24;12(4):676.

[3] Giordani M, Polese M, Mezzavilla M, Rangan S, Zorzi M. Toward 6G networks: Use cases and technologies. IEEE Communications Magazine. 2020 Mar 18;58(3):55-61.

[4] Mahmoud HH, Amer AA, Ismail T. 6G: A comprehensive survey on technologies, applications, challenges, and research problems. Transactions on Emerging Telecommunications Technologies. 2021 Apr;32(4):e4233.

[5] De Alwis C, Kalla A, Pham QV, Kumar P, Dev K, Hwang WJ, Liyanage M. Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. IEEE Open Journal of the Communications Society. 2021 Apr 7;2:836-86.

[6] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Feb 8:103117.

[7] You X, Wang CX, Huang J, Gao X, Zhang Z, Wang M, Huang Y, Zhang C, Jiang Y, Wang J, Zhu M. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Science China Information Sciences. 2021 Jan;64:1-74.

[8] Chowdhury MZ, Shahjalal M, Ahmed S, Jang YM. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. IEEE Open Journal of the Communications Society. 2020 Jul 20;1:957-75.

[9] Porambage P, Gür G, Osorio DP, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society. 2021 May 10;2:1094-122.

[10] Guo H, Li J, Liu J, Tian N, Kato N. A survey on space-air-ground-sea integrated network security in 6G. IEEE Communications Surveys & Tutorials. 2021 Nov 30;24(1):53-87.

[11] Alsharif MH, Kelechi AH, Yahya K, Chaudhry SA. Machine learning algorithms for smart data analysis in internet of things environment: taxonomies and research trends. Symmetry. 2020 Jan 2;12(1):88.

[12] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[13] Series M. IMT Vision–Framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation ITU. 2015 Sep;2083(0).

[14] Letaief KB, Chen W, Shi Y, Zhang J, Zhang YJ. The roadmap to 6G: AI empowered wireless networks. IEEE communications magazine. 2019 Aug 21;57(8):84-90.

[15] Chen S, Liang YC, Sun S, Kang S, Cheng W, Peng M. Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed. IEEE Wireless Communications. 2020 Feb 19;27(2):218-28.

[16] Elmeadawy S, Shubair RM. Enabling technologies for 6G future wireless communications: Opportunities and challenges. arXiv preprint arXiv:2002.06068. 2020 Feb 14.

[17] Chen Y, Zhu P, He G, Yan X, Baligh H, Wu J. From connected people, connected things, to connected intelligence. In2020 2nd 6G wireless summit (6G SUMMIT) 2020 Mar 17 (pp. 1-7). IEEE.

[18] Lu Y, Ning X. A vision of 6G–5G's successor. Journal of Management Analytics. 2020 Jul 2;7(3):301-20.

[19] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[20] Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, Karagiannidis GK, Fan P. 6G wireless networks: Vision, requirements, architecture, and key technologies. IEEE Vehicular Technology Magazine. 2019 Jul 18;14(3):28-41.

[21] Alghamdi R, Alhadrami R, Alhothali D, Almorad H, Faisal A, Helal S, Shalabi R, Asfour R, Hammad N, Shams A, Saeed N. Intelligent surfaces for 6G wireless networks: A survey of optimization and performance analysis techniques. IEEE access. 2020 Oct 19;8:202795-818.

[22] Mahbas AJ, Zhu H, Wang J. Impact of small cells overlapping on mobility management. IEEE Transactions on Wireless Communications. 2019 Jan 8;18(2):1054-68.

[23] Chowdhury MZ, Hossan MT, Hasan MK, Jang YM. Integrated RF/optical wireless networks for improving QoS in indoor and transportation applications. Wireless Personal Communications. 2019 Aug 15;107(3):1401-30.

[24] Chowdhury MZ, Hasan MK, Shahjalal M, Hossan MT, Jang YM. Optical wireless hybrid networks: Trends, opportunities, challenges, and research directions. IEEE Communications Surveys & Tutorials. 2020 Jan 15;22(2):930-66.

[25] Hossan MT, Chowdhury MZ, Shahjalal M, Jang YM. Human bond communication with head-mounted displays: scope, challenges, solutions, and applications. IEEE communications magazine. 2019 Feb 21;57(2):26-32.

[26] Stoica RA, de Abreu GT. 6G: the wireless communications network for collaborative and AI applications. arXiv preprint arXiv:1904.03413. 2019 Apr 6.

[27] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[28] Tekbıyık K, Ekti AR, Kurt GK, Görçin A. Terahertz band communication systems: Challenges, novelties and standardization efforts. Physical Communication. 2019 Aug 1;35:100700.

[29] Akyildiz IF, Jornet JM, Han C. Terahertz band: Next frontier for wireless communications. Physical communication. 2014 Sep 1;12:16-32.

[30] Strinati EC, Barbarossa S, Gonzalez-Jimenez JL, Ktenas D, Cassiau N, Maret L, Dehos C. 6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication. IEEE Vehicular Technology Magazine. 2019 Aug 8;14(3):42-50.

[31] Rappaport TS, Xing Y, Kanhere O, Ju S, Madanayake A, Mandal S, Alkhateeb A, Trichopoulos GC. Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond. IEEE access. 2019 Jun 6;7:78729-57.

[32] Akyildiz IF, Kak A, Nie S. 6G and beyond: The future of wireless communications systems. IEEE access. 2020 Jul 21;8:133995-4030.

[33] Lovén L, Leppänen T, Peltonen E, Partala J, Harjula E, Porambage P, Ylianttila M, Riekki J. EdgeAI: A vision for distributed, edge-native artificial intelligence in future 6G networks. The 1st 6G wireless summit. 2019 Mar:1-2.

[34] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[35] Clazzer F, Munari A, Liva G, Lazaro F, Stefanovic C, Popovski P. From 5G to 6G: Has the time for modern random access come?. arXiv preprint arXiv:1903.03063. 2019 Mar 1.

[36] Mahmood NH, Alves H, López OA, Shehab M, Osorio DP, Latva-Aho M. Six key features of machine type communication in 6G. In2020 2nd 6G Wireless Summit (6G SUMMIT) 2020 Mar 17 (pp. 1-5). IEEE.

[37] Zhao J. A survey of intelligent reflecting surfaces (IRSs): Towards 6G wireless communication networks. arXiv preprint arXiv:1907.04789. 2019 Jul 8.

[38] Pan C, Yi J, Yin C, Yu J, Li X. Joint 3D UAV placement and resource allocation in software-defined cellular networks with wireless backhaul. IEEE Access. 2019 Jul 10;7:104279-93.

[39] Mozaffari M, Kasgari AT, Saad W, Bennis M, Debbah M. Beyond 5G with UAVs: Foundations of a 3D wireless cellular network. IEEE Transactions on Wireless Communications. 2018 Nov 13;18(1):357-72.

[40] Dang S, Amin O, Shihada B, Alouini MS. What should 6G be?. Nature Electronics. 2020 Jan;3(1):20-9.

[41] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[42] Gao H, Su Y, Zhang S, Diao M. Antenna selection and power allocation design for 5G massive MIMO uplink networks. China Communications. 2019 Apr 22;16(4):1-5.

[43] Attarifar M, Abbasfar A, Lozano A. Modified conjugate beamforming for cell-free massive MIMO. IEEE Wireless Communications Letters. 2019 Jan 1;8(2):616-9.

[44] Wang H, Wang W, Chen X, Zhang Z. Wireless information and energy transfer in interference aware massive MIMO systems. In2014 IEEE Global Communications Conference 2014 Dec 8 (pp. 2556-2561). IEEE.

[45] Elmeadawy S, Shubair RM. 6G wireless communications: Future technologies and research challenges. In2019 international conference on electrical and computing technologies and applications (ICECTA) 2019 Nov 19 (pp. 1-5). IEEE.

[46] Henry R, Herzberg A, Kate A. Blockchain access privacy: Challenges and directions. IEEE Security & Privacy. 2018 Aug 6;16(4):38-45.

[47] Aste T, Tasca P, Di Matteo T. Blockchain technologies: The foreseeable impact on society and industry. Computer. 2017 Jan50(9): 18–28.

[48] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432).

[49] Miller D. Blockchain and the internet of things in the industrial sector. IT professional. 2018 Jun 11;20(3):15-8.

[50] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications. 2020 Sep 15;166:102693.

[51] Nguyen T, Tran N, Loven L, Partala J, Kechadi MT, Pirttikangas S. Privacy-aware blockchain innovation for 6G: Challenges and opportunities. 2020 2nd 6G Wireless Summit (6G SUMMIT). 2020 Mar 17:1-5.

[52] Dai HN, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal. 2019 Jun 5;6(5):8076-94.

[53] Taleb T, Samdanis K, Mada B, Flinck H, Dutta S, Sabella D. On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Communications Surveys & Tutorials. 2017 May 18;19(3):1657-81.

[54] Huang T, Yang W, Wu J, Ma J, Zhang X, Zhang D. A survey on green 6G network: Architecture and technologies. IEEE access. 2019 Dec 4;7:175758-68.

[55] Huang X, Zhang JA, Liu RP, Guo YJ, Hanzo L. Airplane-aided integrated networking for 6G wireless: Will it work?. IEEE Vehicular Technology Magazine. 2019 Jul 12;14(3):84-91.

[56] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[57] Giordani M, Zorzi M. Satellite communication at millimeter waves: A key enabler of the 6G era. In2020 International Conference on Computing, Networking and Communications (ICNC) 2020 Feb 17 (pp. 383-388). IEEE.

[58] Höyhtyä M, Martio J. Integrated satellite–terrestrial connectivity for autonomous ships: Survey and future research directions. Remote Sensing. 2020 Aug 4;12(15):2507.

[59] Tariq F, Khandaker MR, Wong KK, Imran MA, Bennis M, Debbah M. A speculative study on 6G. IEEE Wireless Communications. 2020 Aug 18;27(4):118-25.

[60] Popovski P, Trillingsgaard KF, Simeone O, Durisi G. 5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view. Ieee Access. 2018 Sep 28;6:55765-79.

[61] Menouar H, Guvenc I, Akkaya K, Uluagac AS, Kadri A, Tuncer A. UAV-enabled intelligent transportation systems for the smart city: Applications and challenges. IEEE Communications Magazine. 2017 Mar 13;55(3):22-8.

[62] Deebak BD, Al-Turjman F. Drone of IoT in 6G wireless communications: Technology, challenges, and future aspects. Unmanned Aerial Vehicles in Smart Cities. 2020:153-65.

[63] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[64] Zhu X, Jiang C. Integrated satellite-terrestrial networks toward 6G: Architectures, applications, and challenges. IEEE Internet of Things Journal. 2021 Nov 10;9(1):437-61.

[65] Petrov I, Janevski T. 5G mobile technologies and early 6G viewpoints. European Journal of Engineering and Technology Research. 2020 Oct 14;5(10):1240-6.

[66] Yang H, Alphones A, Xiong Z, Niyato D, Zhao J, Wu K. Artificial-intelligence-enabled intelligent 6G networks. IEEE Network. 2020 Oct 23;34(6):272-80.

[67] Siriwardhana Y, Porambage P, Liyanage M, Ylianttila M. A survey on mobile augmented reality with 5G mobile edge computing: architectures, applications, and technical aspects. IEEE Communications Surveys & Tutorials. 2021 Feb 25;23(2):1160-92.

[68] Peltonen E, Bennis M, Capobianco M, Debbah M, Ding A, Gil-Castiñeira F, Jurmu M, Karvonen T, Kelanti M, Kliks A, Leppänen T. 6G white paper on edge intelligence. arXiv preprint arXiv:2004.14850. 2020 Apr 30.

[69] Peltonen E, Bennis M, Capobianco M, Debbah M, Ding A, Gil-Castiñeira F, Jurmu M, Karvonen T, Kelanti M, Kliks A, Leppänen T. 6G white paper on edge intelligence. arXiv preprint arXiv:2004.14850. 2020 Apr 30.

[70] Shahinzadeh H, Moradi J, Gharehpetian GB, Nafisi H, Abedi M. Internet of Energy (IoE) in smart power systems. In2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI) 2019 Feb 28 (pp. 627-636). IEEE.

[71] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep;33(9):e4528.

[72] Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG. A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Communications Surveys & Tutorials. 2020 Apr 14;22(3):1942-76.

[73] Nayak S, Patgiri R. 6G communication technology: A vision on intelligent healthcare. Health informatics: A computational perspective in healthcare. 2021:1-8.

[74] Mucchi L, Jayousi S, Caputo S, Paoletti E, Zoppi P, Geli S, Dioniso P. How 6G technology can change the future wireless healthcare. In2020 2nd 6G wireless summit (6G SUMMIT) 2020 Mar 17 (pp. 1-6). IEEE.

[75] Grieves M, Vickers J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Transdisciplinary perspectives on complex systems: New findings and approaches. 2017:85-113.

[76] Grieves MW. Virtually intelligent product systems: Digital and physical twins. American Institute of Aeronautics and Astronautics. 2019:175-200

[77] Hewa T, Ylianttila M, Liyanage M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications. 2021 Mar 1;177:102857.

[78] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[79] Saad W, Bennis M, Chen M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE network. 2019 Oct 16;34(3):134-42.

[80] Yu Q, Zhou H, Chen J, Li Y, Jing J, Zhao JJ, Qian B, Wang J. A fully-decoupled RAN architecture for 6G inspired by neurotransmission. Journal of Communications and Information Networks. 2019 Dec;4(4):15-23.

[81] Bhat JR, Alqahtani SA. 6G ecosystem: Current status and future perspective. IEEE Access. 2021 Jan 26;9:43134-67.

[82] Mahmood NH, Alves H, López OA, Shehab M, Osorio DP, Latva-Aho M. Six key features of machine type communication in 6G. In2020 2nd 6G Wireless Summit (6G SUMMIT) 2020 Mar 17 (pp. 1-5). IEEE.

[83] Zhao Y, Yu G, Xu H. 6G mobile communication network: vision, challenges and key technologies. arXiv preprint arXiv:1905.04983. 2019 May 3.

[84] Zioga P, Pollick F, Ma M, Chapman P, Stefanov K. “Enheduanna—a Manifesto of Falling” live brain-computer cinema performance: performer and audience participation, cognition and emotional engagement using multi-brain BCI interaction. Frontiers in neuroscience. 2018 Apr 3;12:191.

[85] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[86] Khan LU, Yaqoob I, Imran M, Han Z, Hong CS. 6G wireless systems: A vision, architectural elements, and future directions. IEEE access. 2020 Aug 10;8:147029-44.

[87] Wang M, Zhu T, Zhang T, Zhang J, Yu S, Zhou W. Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks. 2020 Aug 1;6(3):281-91.

[88] Liyanage M, Abro AB, Ylianttila M, Gurtov A. Opportunities and challenges of software-defined mobile networks in network security. IEEE security & privacy. 2016 Aug 5;14(4):34-44.

[89] Khan R, Kumar P, Jayakody DN, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials. 2019 Aug 8;22(1):196-248.

[90] Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A. Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine. 2018 Apr 11;2(1):36-43.

[91] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[92] Sicari S, Rizzardi A, Coen-Porisini A. 5G In the internet of things era: An overview on security and privacy challenges. Computer Networks. 2020 Oct 9;179:107345.

[93] Ranaweera P, Jurcut AD, Liyanage M. Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials. 2021 Feb 26;23(2):1078-124.

[94] Chohan UW. The double spending problem and crypto-currencies. SSRN Electron. 2021 Mar:1

[95] Zhang S, Lee JH. Double-spending with a sybil attack in the bitcoin decentralized network. IEEE transactions on Industrial Informatics. 2019 Jun 10;15(10):5715-22.

[96] Mehar MI, Shier CL, Giambattista A, Gong E, Fletcher G, Sanayhie R, Kim HM, Laskowski M. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. Journal of Cases on Information Technology (JCIT). 2019 Jan 1;21(1):19-32.

[97] Otte P, de Vos M, Pouwelse J. TrustChain: A Sybil-resistant scalable blockchain. Future Generation Computer Systems. 2020 Jun 1;107:770-80.

[98] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[99] Feng Q, He D, Zeadally S, Khan MK, Kumar N. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications. 2019 Jan 15;126:45-58.

[100] Bünz B, Agrawal S, Zamani M, Boneh D. Zether: Towards privacy in a smart contract world. InFinancial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 2020 Jul 18 (pp. 423-443). Cham: Springer International Publishing.

[101] Dorri A, Steger M, Kanhere SS, Jurdak R. Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine. 2017 Dec 13;55(12):119-25.

[102] Bao Z, Wang Q, Shi W, Wang L, Lei H, Chen B. When blockchain meets sgx: An overview, challenges, and open issues. IEEE Access. 2020 Sep 15;8:170404-20.

[103] Xiao H, Biggio B, Brown G, Fumera G, Eckert C, Roli F. Is feature selection secure against training data poisoning?. Ininternational conference on machine learning 2015 Jun 1 (pp. 1689-1698). PMLR.

[104] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[105] Khurana N, Mittal S, Piplai A, Joshi A. Preventing poisoning attacks on ai based threat intelligence systems. In2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP) 2019 Oct 13 (pp. 1-6). IEEE.

[106] Pawlicki M, Choraś M, Kozik R. Defending network intrusion detection systems against adversarial evasion attacks. Future Generation Computer Systems. 2020 Sep 1;110:148-54.

[107] Arfaoui MA, Soltani MD, Tavakkolnia I, Ghrayeb A, Safari M, Assi CM, Haas H. Physical layer security for visible light communication systems: A survey. IEEE Communications Surveys & Tutorials. 2020 Apr 17;22(3):1887-908.

[108] Benzaid C, Taleb T. ZSM security: Threat surface and best practices. IEEE Network. 2020 Feb 12;34(3):124-33.

[109] Ortiz J, Sanchez-Iborra R, Bernabe JB, Skarmeta A, Benzaid C, Taleb T, Alemany P, Muñoz R, Vilalta R, Gaber C, Wary JP. INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks. InProceedings of the 15th International Conference on Availability, Reliability and Security 2020 Aug 25 (pp. 1-10).

[110] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[111] Siriwardhana Y, Porambage P, Liyanage M, Ylianttila M. AI and 6G security: Opportunities and challenges. In2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) 2021 Jun 8 (pp. 616-621). IEEE.

[112] Sanchez-Navarro I, Salva-Garcia P, Wang Q, Calero JM. New immersive interface for zero-touch management in 5G networks. In2020 IEEE 3rd 5G World Forum (5GWF) 2020 Sep 10 (pp. 145-150). IEEE.

[113] Hyder MF, Ismail MA. INMTD: Intent-based moving target defense framework using software defined networks. Engineering, Technology & Applied Science Research. 2020 Feb 3;10(1):5142-7.

[114] Han Y, Li J, Hoang D, Yoo JH, Hong JW. An intent-based network virtualization platform for SDN. In2016 12th International Conference on Network and Service Management (CNSM) 2016 Oct 31 (pp. 353-358). IEEE.

[115] Wei Y, Peng M, Liu Y. Intent-based networks for 6G: Insights and challenges. Digital Communications and Networks. 2020 Aug 1;6(3):270-80.

[116] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[117] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok). InPrinciples of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6 2017 (pp. 164-186). Springer Berlin Heidelberg.

[118] Wohrer M, Zdun U. Smart contracts: security patterns in the ethereum ecosystem and solidity. In2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) 2018 Mar 20 (pp. 2-8). IEEE.

[119] Liu C, Liu H, Cao Z, Chen Z, Chen B, Roscoe B. Reguard: finding reentrancy bugs in smart contracts. InProceedings of the 40th International Conference on Software Engineering: Companion Proceeedings 2018 May 27 (pp. 65-68).

[120] Jiang B, Liu Y, Chan WK. Contractfuzzer: Fuzzing smart contracts for vulnerability detection. InProceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering 2018 Sep 3 (pp. 259-269).

[121] Brent L, Jurisevic A, Kong M, Liu E, Gauthier F, Gramoli V, Holz R, Scholz B. Vandal: A scalable security analysis framework for smart contracts. arXiv preprint arXiv:1809.03981. 2018 Sep 11.

[122] Bhargavan K, Delignat-Lavaud A, Fournet C, Gollamudi A, Gonthier G, Kobeissi N, Kulatova N, Rastogi A, Sibut-Pinote T, Swamy N, Zanella-Béguelin S. Formal verification of smart contracts: Short paper. InProceedings of the 2016 ACM workshop on programming languages and analysis for security 2016 Oct 24 (pp. 91-96).

[123] Abdellatif T, Brousmiche KL. Formal verification of smart contracts based on users and blockchain behaviors models. In2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2018 Feb 26 (pp. 1-5). IEEE.

[124] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[125] Schaar P. Privacy by design. Identity in the Information Society. 2010 Aug;3(2):267-74.

[126] Cavoukian A. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada. 2009 Aug;5:12.

[127] Cheng R, Zhang F, Kos J, He W, Hynes N, Johnson N, Juels A, Miller A, Song D. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In2019 IEEE European Symposium on Security and Privacy (EuroS&P) 2019 Jun 17 (pp. 185-200). IEEE.

[128] Yuan R, Xia YB, Chen HB, Zang BY, Xie J. Shadoweth: Private smart contract on public blockchain. Journal of Computer Science and Technology. 2018 May;33:542-56.

[129] Weerasinghe N, Hewa T, Liyanage M, Kanhere SS, Ylianttila M. A novel blockchain-as-a-service (BaaS) platform for local 5G operators. IEEE Open Journal of the Communications Society. 2021 Mar 19;2:575-601.

[130] Lohachab A, Lohachab A, Jangra A. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things. 2020 Mar 1;9:100174.

[131] Tramèr F, Kurakin A, Papernot N, Goodfellow I, Boneh D, McDaniel P. Ensemble adversarial training: Attacks and defenses. arXiv preprint arXiv:1705.07204. 2017 May 19.

[132] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[133] Soll M, Hinz T, Magg S, Wermter S. Evaluating defensive distillation for defending text processing neural networks against adversarial examples. InArtificial Neural Networks and Machine Learning–ICANN 2019: Image Processing: 28th International Conference on Artificial Neural Networks, Munich, Germany, September 17–19, 2019, Proceedings, Part III 28 2019 (pp. 685-696). Springer International Publishing.

[134] Li W, Su Z, Li R, Zhang K, Wang Y. Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Network. 2020 Dec 2;34(6):31-7.

[135] Roy A, Chhabra A, Kamhoua CA, Mohapatra P. A moving target defense against adversarial machine learning. InProceedings of the 4th ACM/IEEE Symposium on Edge Computing 2019 Nov 7 (pp. 383-388).

[136] Sengupta S, Chakraborti T, Kambhampati S. Mtdeep: boosting the security of deep neural nets against adversarial attacks with moving target defense. InDecision and Game Theory for Security: 10th International Conference, GameSec 2019, Stockholm, Sweden, October 30–November 1, 2019, Proceedings 10 2019 (pp. 479-491). Springer International Publishing.

[137] Liu J, Chen L, Miné A, Wang J. Input validation for neural networks via runtime local robustness verification. arXiv preprint arXiv:2002.03339. 2020 Feb 9.

[138] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6).

[139] Li B, Chen C, Wang W, Carin L. Certified adversarial robustness with additive noise. Advances in neural information processing systems. 2019;32.

[140] Petrov V, Moltchanov D, Jornet JM, Koucheryavy Y. Exploiting multipath terahertz communications for physical layer security in beyond 5G networks. InIEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2019 Apr 29 (pp. 865-872). IEEE.

[141] Rahman MM, Abbasi QH, Chopra N, Qaraqe K, Alomainy A. Physical layer authentication in nano networks at terahertz frequencies for biomedical applications. IEEE Access. 2017 May 2;5:7808-15.

[142] Mostafa A, Lampe L. Physical-layer security for indoor visible light communications. In2014 IEEE International Conference on Communications (ICC) 2014 Jun 10 (pp. 3342-3347). IEEE.

[143] Fawaz HI, Forestier G, Weber J, Idoumghar L, Muller PA. Adversarial attacks on deep neural networks for time series classification. In2019 International Joint Conference on Neural Networks (IJCNN) 2019 Jul 14 (pp. 1-8). IEEE.

[144] Liu J, Chen L, Miné A, Wang J. Input validation for neural networks via runtime local robustness verification. arXiv preprint arXiv:2002.03339. 2020 Feb 9.