Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 8, August 2021, pg.8 – 14

Edge Computing and Its Convergence with Blockchain in 6G: Security Challenges

Alex Mathew[1]
[1]Bethany College, USA
DOI: 10.47760/ijcsmc.2021.v10i08.002

Abstract— Even though the wireless network of 5G has not been investigated exhaustively, the sixth generation (6G) echo systems' visionaries are already being debated. Therefore, to solidify and consolidate privacy and security within 6G networks, this paper examines edge computing and its convergence with blockchain in 6G: security challenges. Moreover, the paper examines how security might affect the wireless systems of the 6G, potential obstacles characterizing various 6G technologies, alongside possible remedies. This paper unveils the 6G security vision alongside key indicators of performance with tentative landscape threat premised upon predicted sixth generation infrastructure. Furthermore, a discussion of the privacy and security challenges that might emerge from the existing sixth generation applications and demands is presented. Additionally, the paper sheds light into the research-level projects and standardization efforts. Specific attention is accorded to discussion on the security consideration with 6G enhancing technologies, including quantum computing, visible light communication (VLC), distributed ML/AI, physical layer security, and distributed ledger technology (DLT). Overall, this paper seeks to guide the subsequent investigation of sixth generation privacy and security in the early stage of envisioning to practicality.
Keywords— Quantum computing, Privacy, Physical Layer Security, ML/AI security, Security threats, Security, 6G

I. INTRODUCTION

The transformation of mobile communication technology began from the 1G cellular networks during the 80s. Since that time, considerable developments are incorporated into the networking and telecommunication industry to cater for 3G, 4G and 2G networks. Since 2020, the 5G mobile technologies' era is within the implementation stage and its evolution has not been undertaken on software-driven networks. Network cloudification with the micro service-oriented infrastructure constitutes the most striking feature of 5G. This offers physical resource abstraction to logical and virtual settings unveiling on-demand automated learning management function. Although 5G coverage is yet to be availed fully, researchers are already envisioning the sixth generation (6G) mobile communication. Although

expectations reveal that the roll out of 6G standardization will commence in 2030, the research fraternity has already begun seeking novel research guides to actualizing sixth generation vision [1]. Communication and networking scientific community anticipate that intelligent network management and orchestration will entirely drive sixth generation wireless networks [2], [3]. This will be achieved using different technologies including quantum computing, cell-free communications, electromagnetic–orbital angular momentum, visible light communications (VLC), re-configurable intelligent surfaces (RIS)[4].The driving aspect of 5G evolution, including cloudified core networks and virtual radio access networks project the premise of 6Ginfrastructural framework. As indicated in [5], 6G is undergoing evolution on orchestration, specializations, functional infrastructure, and platform. Concerning the platforms, cloudification of heterogeneous architecture is anticipated within sixth generation infrastructure to attain maximal execution of Network Function (NF) [6].The process requires the capacity for locating the services, which several clouds provide alongside placement of continuous functions. Functional infrastructures necessitate emerging functions that include, but not restricted to information gathering, RAN-core integration and cell-free radios for artificial intelligence at management or physical layers. Novel specialization mechanisms are also expected including offloading flexible workload, extreme slicing, and personal sub-networks [7]. During 6G cognitive network management, the cognitive automation and closed loop form the basis for orchestration.

The privacy and security considerations within the envisioned sixth generation network should be tackled in terms of multiple areas. As indicated earlier, novel 6G infrastructural framework is characterized by specific security concerns. Besides, numerous hypes exist on novel technology blending, such as quantum computing, TeraHertz (THz), VLC, and blockchain features within 6G intelligent networking paradigm for tackling privacy and security concerns. Therefore, security considerations of 6G must also be debated in terms of deep learning security, application security, network information security and physical layer security [4].

A. Evolution of Mobile Security

Previous mobile network generations (that is, 3G, 2G, and 1G) grappled with several privacy and security challenges including privacy issues, authorization and authentication problems, encryption issues, eavesdropping, unauthorized physical attacks, and cloning [5]. Then, the landscape of security threats has undergone evolution with more powerful attackers and sophisticated attack situations. Figure 1 shows the security landscape evolution of telecommunication network, from fourth generation to the envisioned sixth generation.

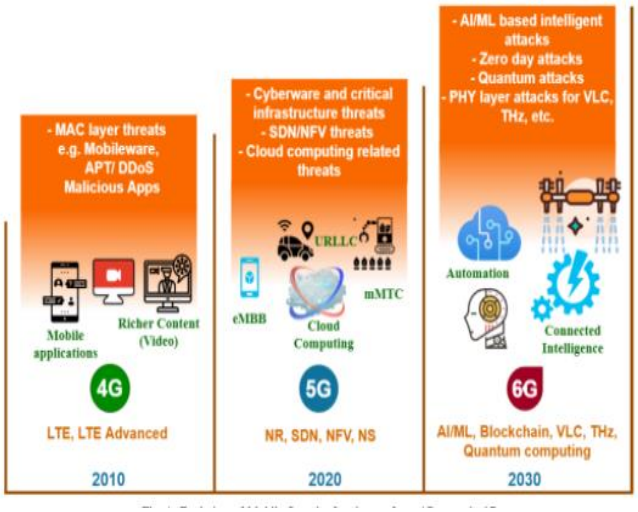

Figure 1: Wireless Security Landscapes' Evolution from 4G to 6G

Fourth generation networks encountered privacy and security threats arising from wireless application execution. Typical cases include malware applications (e.g., hardware tampering, viruses), and media access control (MAC) layer security threats (e.g., replay attacks, eavesdropping, denial of service (DoS) attacks. In the fifth infrastructure, privacy and security exist at core, backhaul and access networks [10]. In 5G, common security concerns include cloud computing threats, Software Defined Networking (SDN), Network Function Virtualization (NFV) and critical infrastructure and cyberware threats [11]. Several scenarios where SDN can present security issues exist, including through network centralization, openflow inception, and exposure of crucial Application Programming Interface (API) towards unexpected software [12]. Overall, additional linked intelligence within a

telecommunication network characterized by ML/AI technologies alongside advanced networking constitutes the main driver in sixth generation vision. Nevertheless, the alliance involving 6G and AI may also act as a double-edged sword in numerous scenarios while seeking for infringing or protecting privacy and security [13].

B. Motivation

Regardless of communication and networking technology advancements, security constitutes a core feature worth considering ensuring the network reliability and resilience. Therefore, it is imperative for the research fraternity to locate research directions related to security within the envisioned sixth generation networks. Since the specifications and standard functions of 6G have not been explained, there is still limited literature, which offers privacy and security insights beyond 5G network.

C. The Contributions of the paper

Because the sixth generation network has not been discovered, it is important to investigate its privacy and security elements from various perspectives. Thus, this paper will attempt to assemble upcoming study guides within 6G security and compare their evolution with existing research. Key contributions within the paper include:

- **Exploring enabling technologies and driving requirements, applications, visions, and trends linked to 6G privacy and security.**
- **Identifying threat landscapes and potential solutions for 6G on distributed ML/AI, quantum communication, physical layer security, and distributed ledger technology (DLT)**
- **Presenting a plan for actualizing 6G security vision.**

II. SECURITY ISSUES FACING SIXTH GENERATION APPLICATIONS

Sixth generation networks have emerged as facilitators of network towards various applications that will drastically redefine the 2030s human society and beyond. Nevertheless, such services and applications have challenging performance needs and extremely strict security thresholds because of the needs for high levels of trust and importance. The relationship between the security requirements and performance expectations increases complexity with the rise of nefarious activities and ubiquitous and capable attackers. The envisaged capacity of 6G can help several potential use cases and novel applications. Figure 2 recaps several influential 6G applications to explain the considerations of security. These applications are considered as initial deployment applications and use cases of 6G in the existing research literature [14]. Figure 3 represents the major security challenges of Blockchanized 6G services.

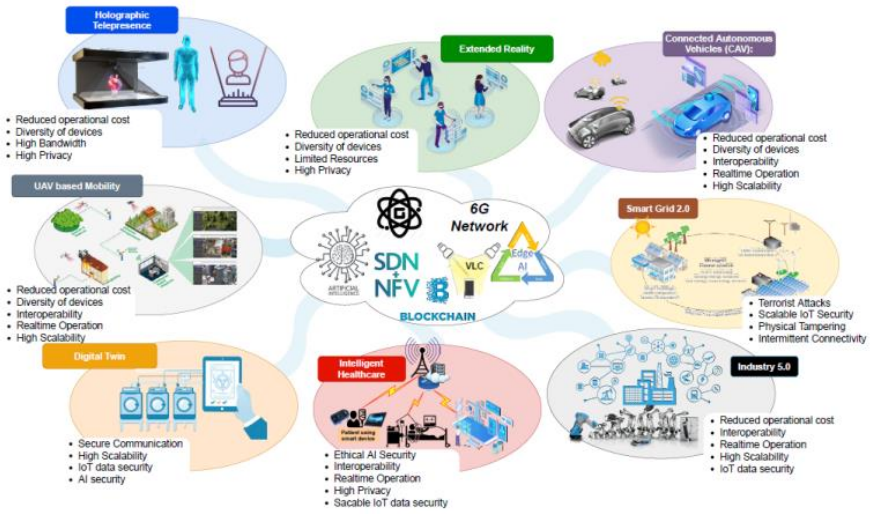

Figure 2: Critical Security Challenges of 6G Applications

Figure 3: Major security challenges of Blockchanized 6G services

III. EDGE COMPUTING AND BLOCKCHAIN

The emerging edge computing and blockchain technologies have showed reliable properties, which can handle the issues mentioned earlier in the paper. This section explains how both technologies function in addressing the issues.

A. Block chain

Blockchains refer to secure and distributed ledgers that record the transactions in hierarchically expanding block chains [10], [11]. All blocks within the blockchain are connected to previous blocks via the parent block's hash value, except the initial block that lacks parent blocks. Emerging blocks may be committed towards blockchains solely after completing the competitions that consensus algorithms enforced.

B. Edge Computing

Centralized cloud computing has become complex to fulfill several quality-of-service (QoS) demands of different applications due to the drastic rise in the quantity of IIoT/IoT devices [12]. The introduction of edge computing is intended to enhance proximity between computation tasks and computational capability, and in turn preserve bandwidth resources and decrease network latency [13].

IV. METHODOLOGY

Recognizing that 6G is still in the initial development and research, a quest for supporting 6G development and research decision-making in industry and government has surfaced. Despite massive economic and technologic uncertainties, investigation concerning how possible 6G rollouts may be achieved temporally and spatially remains at the policy formulation phase. Thus, implications of 6G network rollout, cost, and coverage across the globe are examined through extrapolation of 5G properties. In this paper, the focus is on a reliable methodology, which covers 6G connectivity alongside its effect of the end user speeds, infrastructure sharing, and annual capital intensity. Furthermore, by incorporating current and new spectra, 6G networks capable of attaining Tera Bit speed with low latency and significant network capacity are envisioned for free service across the world.

Sequential methodology [14], Ref. [15] (p. 639) processes helps analysis teams to describe the conditions, then plan for designs before execution and focus on network spectrum and densification. To increase the performance of 6G system experiments, the sequential approach is capable of exploiting novel adaptive techniques of different applications locating the future directions within the development and research field. Figures 4a, b shows the sequential methodology of the 6GIIoE system.

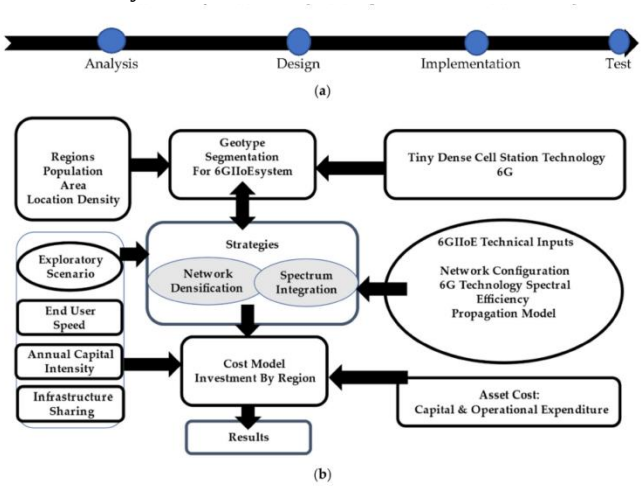

Figure 4: (a) Phase by phase sequential methodology process. (b) Sequential Methodology Process

V. ARCHITECTURAL FRAMEWORK OF 6GIIOE

The reference architectures, specifications, and literature review thresholds (particularly) of 6G IIoE systems do not exist. Researchers are working hard to design 6G specifications and standards. From this perspective, it is envisioned that 6G specifications and standards will be introduced before 2030. Sixth generation communication infrastructure must enable internet connection and autonomous communication for IIoE machines, sensors, and devices.

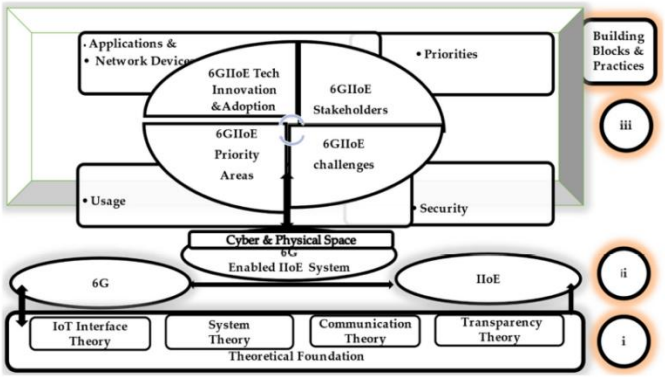

Figure 5: A Novel Theoretical Framework

VI. RESULTS

This section offers substantive simulation outcomes for evaluating the performance of 6G based on the convergence of edge computing and blockchain. To provide a comprehensive method, numerous experimental tests were conducted using different performance metrics. Performance was analyzed based on latency rate during query transactions, transaction reaction time for several user requests, and resource use analysis. For purposes of evaluation, Postman is utilized to analyze Hyperledger Caliper, APIs, and RESTful. During querying transaction, latency rates include the transaction request submission time and the duration needed for the web clients to approve the request.

6.1. Simulation

Deployment of the test-bed occurs within two different development settings: web application and blockchain. The Hyperledger Composer's online version is deprecated, thus the Hyperledger Composer's offline version is used for the purpose of simulation. The process of installation includes composer playground user interface, starting fabric composers, development environment preparation. Figure 6 below shows the transaction flow diagram between blockchain peers whereas algorithm 1 illustrates the pseudocode for IoT gadget state transaction.

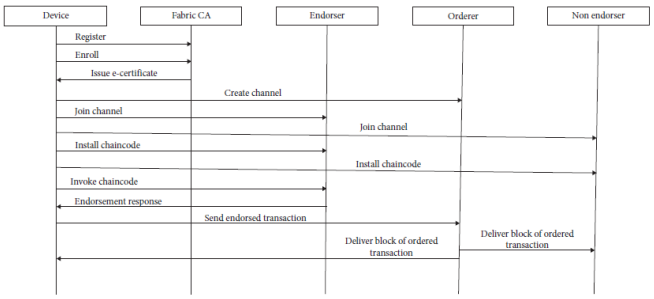

Figure 6: Flow diagram of the transaction between peers of blockchain.

```
Ensure: Initialize var deviceRegistry
Ensure: Initialize var deviceID
Ensure: Initialize var t-list
Ensure: Initialize var station = getstation ()
if tx.newstate = True then
        deviceID.state = tx.newstate
        if tx.enables ! = null then
           deviceID.enabled = tx.enabled }\newline
           dev-station = station }\newline
           t-list = deviceID }\newline
        elseif tx.newstate = False
           event.msg ("State of IoT dvice having ID "+ deviceID +" has not changed")
     end if
  end if
return asset.update (deviceID)
return event.msg ("State of IoT dvice having ID "+ deviceID +" has been changed.") = 0
```

ALGORITHM 1: Pseudocode for IoT device state transaction

VII. CONCLUSIONS

Parallel to 5G wireless system deployments, the research fraternity is unveiling the platform for 6G's wireless communication rollout. Driving the 6G security vision to a reality has started from the study level. Within the paper, the initial survey on 6G privacy and security that covers potential areas, which can be touched using sixth generation security considerations. It originates in a white paper that a telecommunication security team wrote. Sixth generation is still within the earliest stages and standardization is yet to begin with deployment slated for 2030. This paper attempted to locate the threat landscape and appropriate security technologies based on 6G future use cases. Overall, the goal was to assemble a survey that serves as the enlightening guide for 6G security in future research.

REFERENCES

[1] P. Porambage, G. G¨ur, D. P. M. Osorio, Member, M. Liyanage, A. Gurtov, M. Ylianttila, "The Roadmap to 6G Security and Privacy," *in 2021 Joint European Conference on Networks and Communications (EuCNC) and 6G Summit*. IEEE, 2021, pp. 1–6.

[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] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang et al., "Towards 6G wireless communication networks: Vision, + enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 64, no. 1, pp. 1–74, 2021.

[4] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security and intelligence," IEEE Wireless Communications, 2020.

[5] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," Digital Communications and Networks, vol. 6, no. 3, pp. 281–291, 2020.

[6] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[7] P.K., Padhi, F. Charrua-Santos. 6G Enabled Industrial Internet of Everything: Towards a Theoretical Framework. *Appl. Syst. Innov* 4, 11. 2021

[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] B. Schneier, "Artificial intelligence and the attack/defense balance," *IEEE security & privacy*, vol. 16, no. 2, pp. 96–96, 2018.

[10] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[11] J.Xie,H.Tang,T.Huang,F.R.Yu,R.Xie,J.Liu,andY.Liu,"Asurvey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[12] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. R. Choo, and M. Dlodlo, "From cloud to fog computing: A review and a conceptual live vm migration framework," IEEE Access, vol. 5, pp. 8284–8300, 2017.

[13] S. A., Bhat, I. B. Sofi and C-Y Chi. Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities, *Special Section On Blockchain Technology: Principles And Applications*.2020

[14] B. Rojas, C. Bolaños, R. Salazar-Cabrera, G. Ram´ırezGonza´lez, ´A. Pacho´n de la Cruz, and J. M. Madrid Molina, "Fleet management and control system for medium-sized cities based in intelligent transportation systems: from review to proposal in a city," Electronics, vol. 9, no. 9, p.1383, 2020.

[15] A. Balasubramaniam, M. J.J. Gul, V. G. Menon, and A. Paul, "Blockchain for intelligent transport system," IETE Technical Review, pp. 1–12, 2020.

