National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 7, No. 2, 2025 (pp. 44-50)
RESEARCH ARTICLE
WWW.ANTENNAJOURNAL.COM

Improving Security in 5G and Next-Generation Networks Through Blockchain Integration

Ezhilarasan Ganesan[1]*, Trapty Agarwal[2], Jaspreet Sidhu[3], Shubhi Goyal[4], Shashikant Deepak[5], Ebenezar Jebarani M R[6], Prabhat Ku.Sahu[7]

[1]Professor, Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Ramanagara District, Karnataka - 562112, India,
[2]Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India,
[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India.
[4]Quantum University Research Center, Quantum University, Roorkee, Uttarakhand, 247667, India.
[5]Assistant Professor, uGDX, ATLAS SkillTech University, Mumbai, India,
[6]Professor, Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, India,
[7]Associate Professor, Department of Computer Science and Information Technology, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India

KEYWORDS:
5G security,
Blockchain integration,
Network authentication,
Decentralized trust,
Next-generation networks,
IoT, data integrity,
Access control,
Secure communication,
Wireless infrastructure.

ARTICLE HISTORY:

Received 25-02-2025
Revised 31-03-2025
Accepted 30-04-2025

DOI:
https://doi.org/10.31838/NJAP/07.02.09

Abstract

The progression of wireless technologies to 5G and beyond has offered unmatched improvements in speed, latency, and connectivity which enables a wide range of applications from self-driving cars to IoT systems. At the same time, this has increased risks around network security, privacy, and trust management. Centralized security approaches are becoming less effective for next generation networks because of their dynamic, distributed, and high-density characteristics. This paper looks at the use of blockchain technology as a decentralized, immutable solution toward enhancing the security of 5G and subsequent networks. We analyse the issues of secure authentication, trust, control, data control, and transparent power segregation and access control to show how blockchain in question can address them. Moreover, we describe security frameworks and architectures for 5G technologies that incorporate blockchain along with its efficiency, flexibility, pragmatic relevance, and actual implementation. The study concludes with insights into existing challenges and potential research directions necessary to realize secure and resilient next-generation wireless networks.

Author's e-mail id: g.ezhilarasan@jainuniversity.ac.in, trapty@muit.in, jaspreet.sidhu.orp@chitkara.edu.in, shubhi.mathematics@quantumeducation.in, shashikant.deepak@atlasuniversity.edu.in, ebenezarjebarani.ece@sathyabama.ac.in, prabhatsahu@soa.ac.in,

Author's Orcid id: 0000-0002-5335-2347, 0009-0007-4081-4999, 0009-0002-5658-5629, 0009-0001-1684-7324, 0000-0003-0444-6889, 0000-0001-5327-664X, 0000-0002-0460-9783.

How to cite th is article: Ganesan E, Agarwal T, Sidhu J, Goyal S, Deepak S, Jebarani EMR, Ku. Sahu P, Improving Security in 5G and Next-Generation Networks Through Blockchain Integration, National Journal of Antennas and Propagation, Vol. 7, No.2, 2025 (pp. 44-50).

Introduction

Advancements in communication technology have come with the development of 5G and the subsequent generations of wireless networks which offer ultra-reliable low latency communication (URLLC), massive machine-type communication (mMTC), and even enhanced mobile broadband (eMBB).[1] These technologies serve as prerequisites for the development of self-driving vehicles, remote surgery, smart factories, and smart city frameworks. Nevertheless, the acceleration in growth coupled with the complexities of the 5G architecture introduces novel vulnerabilities while augmenting existing compromises on privacy, scalability, and trust management.[3, 8]

The fully distributed security models that have emerged do not succeed in providing ample protection against the classified and diverse problems within the 5G system.[10] The system is also riddled with the problems of single point failures, trust delays, and complicated real time authentication which necessitates the need for more agile transparent forms of security solutions.[5]

Due to reasons mentioned above, cybersecurity experts have been optimizing decentralized communication networks based on blockchain technology to reinforce the existing infrastructure systems.[2] The salient features of 5G infrastructure such as distributed nature, lack of single point of failure, consensus methods and unchangeable policies create frameworks capable of solving the most pressing security issues concerning 5G frameworks.[7, 13] There is heightened endorsement for blockchain to enable self-governed identity systems, distributed sharing, and proficient access control systems that are protected from external manipulation for extensive and diverse network nodes.[9]

This research studies the incorporation of blockchain technology into 5G and wireless communication systems to enhance network security, as noted in references[6] and.[18] It treats main applications, utilization frameworks, corresponding advantages and the technology problems that pose as barriers to success. In this way, it attempts to provide an understanding about building more secure, block chain enabled communication systems that are easier to scale and more secure, adaptable to future requirements and technologies.[21,24]

Security Challenges in 5G and Next-Generation Networks

The architecture of 5G networks and future networks differs from prior generations as it incorporates advanced new services and an improved connectivity framework. This enhancement, however, brings with it a host of new threats.[16] The challenges arise from a growing number of devices that are connected, the distributed nature of services, and the implementation of Software Defined Networking (SDN) and Network Function Virtualization (NFV).[11] One of the weaknesses in the existing network infrastructure is the centralized control structure. This leads to several points of failure or single points of failure (SPoFs), rendering the system vulnerable to DDoS attacks, spoofing, and interception.[13] The wide variety of devices such as IoT sensors, remotely piloted aircraft systems (RPAS), and autonomous vehicles significantly change security expectations, posing challenges to traditional systems.[4, 23]

The fact that 75 billion devices will be connected by the year 205 [15][14] indicates the existence of a possible hurricane of risk or attack surfaces. The speed with which data is transferred increases the possibility of unwanted interception, session hijacking, as well as leakage of sensitive information, especially during cell handovers and user device movement between different cells.[17] These traditional security frameworks are static in nature since they rely solely on perimeter-based defences, placed on access control silos. Such a changing world alongside these dynamic environments would be too much to bear for such frameworks. The needing environment bypasses the limits which existing protocols provide, such as needing real time authentication along with inability to check the integrity boundless nodes. Also, earlier generations security controls such as pre-shared keys and certificate based, are hard to maintaining across devices which require rapid interaction with one another and undergo reset latency.[19, 22]

On top of this, the concept of slicing a network, which contains multi-tenancy partitions, networks built virtually from a real one, adds extra unwelcomed issues. Any breach within one slice can lock all the others together if the blueprint fails in segmentation.[11] Alongside these limits, there is more pressure to bring forward new flexible and responsive security checks alongside architecture countering the diverse elements of five and subsequent generations of networks.

Blockchain Technology and Its Security Benefits

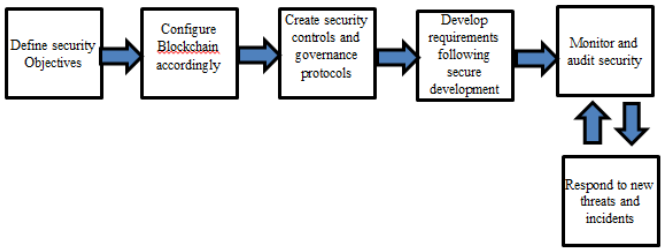

Fig. 1: Blockchain Framework for Security

The provided Figure 1 shows the Blockchain Framework for Security which the authors created to incorporate blockchain securely in 5G networks and further. This process starts from identifying security aims, which include determining important assets, analyzing possible hostile actions, and formulating protection objectives that are compliant with industry rules and government policies. After aims have been set, it is then vital to configure the blockchain to set system architectures, including a permissioned or permissionless system—along with a suitable level of consensus trust and system performance. After this, organizations are required to establish strong security controls and governance structures. This entails defining access control, cryptography policies, and policies governing participation and decision-making at

the node level. Thus, secure development practices are highly emphasized, meaning that within the framework, procedures for design will be to principles of secure software engineering; that is, blockchain applications and smart contracts are crafted to withstand attacks. An area of continuous defense includes the active guarding and verification of the security, meaning monitoring live threats in the system and regular auditing of the system to maintain a healthy operating system. Finally, the framework provides guiding steps to deal with new threats and incidents so that rapid response and ongoing refinement can be achieved. These cycles guarantee that the system operates optimally and adapts target frameworks in which the system is user-friendly for next-generation networks relying on blockchain technology.

A blockchain is a type of boundless ledger technology (LT) which facilitates the distribution of ledgers or records of transactions "across a network of nodes" in a way that ensures easy access to unchangeable information. In addition, any form of alteration or data manipulation attempts is all but infeasible. Every block contains a hash mark of the block that came beforehand, a timestamp that records when the chains were formed, and all transaction details. The feature which is fundamentally set apart from other centralized databases that a blockchain employs is its attribute decentralization. Blockchain does not have a single controlling party which helps reduce the risk of system breaches through unauthorized manipulation, access, failures, or synergetic data breaches which exploit system weaknesses.

From a cyber security perspective, blockchain systems are advantageous. For example, information codification within the blockchain guarantees permanency which enables some work sufficiency in execution audit trails as well as logging, tampering, intrusion, detection of sensitive systems, and sensitive systems' tampering not forgetting subversion. Moreover, the aforementioned along with the onset of fifth generation 5G networks and other most current technologies which position highly on dependably dispersed computing resources makes the form of structure more acceptable and reliable to users. Even more, fortifies the system against DDoS attacks, data breach, and abuse from authorized personnel.

An important additional benefit of security is the use of cryptographic techniques like digital signatures and hash functions. These techniques make it possible to complete data authentication and user identity checking in an automated procedure securely. Furthermore, blockchain facilitates the use of intelligent contracts which are agreements that self-enforce the execution of security measures and conditions in real-time without the involvement of humans. In 5G networks, smart contracts carry out automation pertaining to secure verification of devices, control of access, and allocation of resources.

The security benefits of blockchain have already proven to have significant advantages in many industries. In the finance sector, blockchain is a fundamental technology for cryptocurrencies such as Bitcoin and Ethereum, and it enables secure monetary transactions. In the supply chain industry, businesses track goods on blockchain to prevent counterfeiting and ensure transparency. In the healthcare sector, blockchain allows for the secure sharing of patients' information between healthcare practitioners while ensuring their identity as well as the information's confidentiality and integrity. Having considered these benefits, incorporating blockchain technology into 5G and next generation networks may alleviate current security challenges, thus improving the security of communication infrastructure.

Integration of Blockchain in 5G and Next-Generation Networks

Incorporating blockchain technology into 5G and future networks offers a revolutionary method for addressing security issues which have never been easily addressed before. Enhancing network authentication and authorization systems is one of the effective functions of blockchain. Centralized servers are still implemented in traditional systems for validating identities of devices and managing access control which opens the network to failures and spoofing attacks. On the other hand, blockchain authentication frameworks allocate identity verification to a decentralized ledger. This enables each participant and device to be authenticated through consensus enabling reduced fraudulent identity claims and unauthorized access to the network.

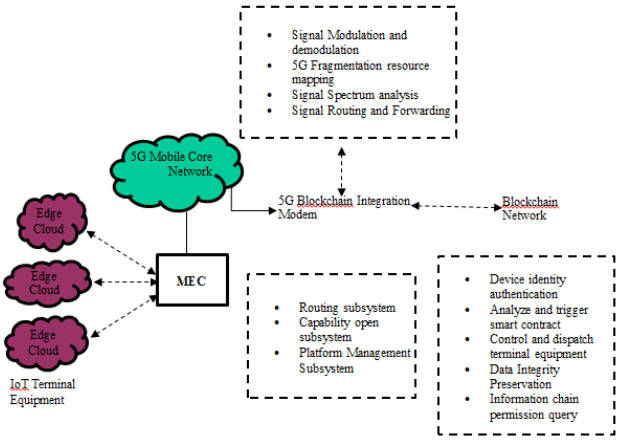

Fig. 2: Blockchain Integration in SG network

Figure 2 gives illustration of a complete system that combines mobile 5G networks with blockchain to improve the security and functionality of IoT ecosystems. At the lowest level, IoT terminal devices, including smart gadgets and sensors, interconnect via access points (APs) to the local edge cloud nodes [20]. These edge clouds are responsible for data processing at lower levels of the network. Lowering the distance to the data source reduces latency and lessens the load on the central network. Routing, capability exposure, subsystem management, and platform administration are some of the important subordinate functions executed at the MEC layer.

Data transmission, signal routing, and modulation is done seamlessly by the 5G Mobile Core Network which serves as the central communication backbone. This core network is connected to the modem that integrates 5G and blockchain, which serves as a link between the traditional network architecture and decentralized blockchain networks. The modem takes care of the devices such as signal modulator/demodulator, resource mapper, spectrum analyzer, and signal relay.

In regard to the blockchain, a distributed network provides the following security measures, including device identity verification, smart contract handling, maintaining data accuracy, and controlled access to information. Moreover, the blockchain can control and manage terminal devices which makes the system highly secure and self-governing. Thus, the system is more secure and can support IoT and 5G technologies in the future in a decentralized manner.

The blockchain permits the efficient and secure transmission and storing of information. It is critical to maintain confidentiality and integrity of the information shared on 5G networks as it is usually sensitive. Encrypted data can be sent over secure networks, placed in fixed vaults using blockchain, and locked away in secure vaults with time markers to ensure any modification is obvious. Moreover, the use of blockchain technology for data storage boosts the system's credibility as it eliminates reliance on a single data store.

Moreover, self-executing contracts, which are self-enforcing agreements placed onto a blockchain, can be employed for automated policy enforcement. In 5G contexts, self-executing contracts may manage the access controls, behaviors, or control permission hierarchies for network resources according to policies set in advance. A self-executing contract may, for example, automatically disconnect a node with an unusual interaction baseline or perform compliance verification at periods defined for inter-device communication. This self-automation removes the burden of manual enforcement of security measures, which is prone to inconsistencies and delays, thus meeting the requirements of 5G networks for ultra-low latency. The integration of blockchain technologies will enhance network infrastructural security by ensuring confidentiality, integrity, and availability, setting a unique 5G architecture for advanced developments in remote medicine, autonomous driving, industrial IoT, and extensive massive IoT smart systems.

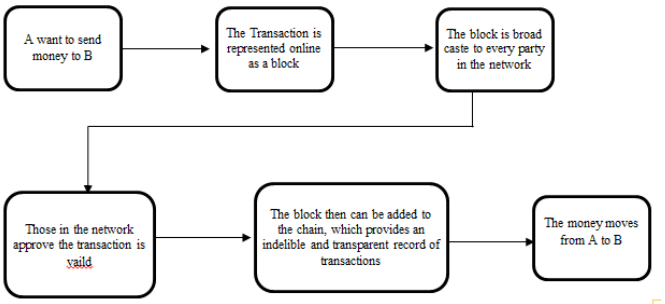

Fig. 3: Blockchain Working Principle

Particularly focusing on the transaction taking place between two users, Figure 3 demonstrates the entire procedure of a blockchain transaction. Firstly, consider user A wishes to send some money to user B. The transaction again is illustrated as a block that contains the user's details including the name of the sender, name of the person receiving the money along with the figures and the time of the transaction. Each block as it is formed must be shared with every single node so every block in the blockchain can check whether this transaction is legitimate or not. These nodes execute control mechanisms like 'proof of work' or 'proof of stake' to collectively approve the transaction that others have confirmed as valid first. The cyclic process put into "blocks" gets appended on the blockchain followed by the addition of the new block securing it forever. As the block gets added on the blockchain it solidifies the transaction confirming that it cannot be changed. Lastly, every user is ensured that the amount is available. The amount A was planning to send to B gets sent safely proving that good faith and confidence is preserved amongst all users as well as among the third-party and everything is managed smoothly without needing central authority intervention, that is truly depicting the foundation and power of blockchain handling.

Pseudocode 1: B5-Sec – Blockchain-Integrated Security Protocol for 5G Networks

Input:

- *Device DiD_iDi with key pair (PKi,SKi)(PK_i, SK_i) (PKi,SKi)*

- *Edge node EEE*
- *Blockchain network BBB*
- *Smart contract SCSCSC*

Output:

- *Securely authenticated and authorized communication session between device and network*

Step 1: Device Registration

```
pseudo
CopyEdit
1. Device D_i generates public-private key
   pair (PK_i, SK_i)
2. D_i → E: {PK_i, Device_ID, Meta_Info}
3. E verifies device credentials and context
4. E → B: Submit transaction to SC for
   device registration
5. SC stores hash(Device_ID, PK_i, Meta_
   Info) on blockchain
```

Step 2: Authentication Phase

```
pseudo
CopyEdit
6. D_i requests session: D_i → E: Session_
   Request
7. E generates nonce N and sends to D_i
8. D_i signs nonce: Sign_SK_i(N) → E
9. E verifies signature using PK_i from
   blockchain
10.If valid: Proceed to session setup
   Else: Reject device
```

Step 3: Session Establishment and Data Transmission

```
pseudo
CopyEdit
11. E and D_i agree on a session key K_s
   using ECDH or similar scheme
12. All data packets P_j sent from D_i:
    For each packet:
    - Timestamp T_j ← current_time
    - Signature ← Sign_SK_i(P_j || T_j)
    - D_i → E: {P_j, T_j, Signature}
13. E verifies timestamp and signature
14. E → B: Log Hash(P_j || T_j) on blockchain
   (optional for audit)
```

Step 4: Continuous Audit and Smart Contract Monitoring

```
pseudo
CopyEdit
15. SC runs scheduled audits:
    If anomaly_behavior(D_i) is detected:
    - SC triggers revocation or quarantine
    - Alert sent to admin node
16. Admin → E: Block D_i or trigger further
    validation
```

Step 5: Session Termination

```
pseudo
CopyEdit
17.  On session end or abnormal activity:
     - Revoke key K_s
     - Log session end with hash(P_final) on
     blockchain
```

Case Studies and Examples

Real-World Applications and Case Studies of Blockchain Integration in Networks

To enhance trust and security, some organizations and leading companies have begun integrating blockchain technology into their 5G and other network infrastructures. For instance, Huawei has been researching blockchain-based network slicing for 5G that facilitate the secure, dynamic resource allocation for diverse users and services. Samsung has also put effort towards blockchain development for securing IoT and device-level data authentication within their smart ecosystems. IBM and Telefónica worked together to add blockchain for inter-carrier network service management and security, which enables secure and streamlined management of roaming agreements and network usage, making it transparent and tamper-proof.

Deutsche Telekom's T-Labs in collaboration with other pilot projects demonstrated how effective blockchain enhances identity spoofing and unauthorized data access for secured identity management across IoT devices. The goal was to decrease the instances of identity spoofing and unauthorized data access. Another example is Jio, an Indian telecom company that integrated a blockchain-based security and tracking framework for device registration and network access, which measurably reduced fraud and increased operational transparency.

As a result of these implementations, multiple lessons and incremental best practices have materialized. One primary lesson emphasizes the need for scalability: blockchain networks must be tuned to manage the extreme transaction throughput in 5G environments without degrading performance. Moreover, organizations need to guarantee the cooperation of other protocols and network standards which usually requires hybrid systems integrating blockchain and traditional database technologies. Moreover, as previously discussed, some

consensus governance frameworks along with delimited regulatory scope are essential to establish credible systems among stakeholders. Following the incremental best practices discussed earlier allows the organizations to harness the prospective benefits of blockchain technology for creating sophisticated, secure, and flexible communication networks.

Challenges and Considerations

The integration of blockchain technology into 5G and future networks indeed offers promising opportunities for enhanced security, but comes with extremely high challenges. One particularly troublesome hurdle is the scalability of blockchain systems. Conventional blockchains, including those used for cryptocurrencies, suffer from low throughput and high latency metrics which simply cannot be accommodated by 5G networks. Adapting blockchain architectures to cope with the requirements of real-time data flow management is a colossal engineering challenge.

Equally restrictive governance structures framework poses significant challenges as well. Radically uncontrolled and pseudonymously managed blocks directly conflict with sovereignty over policy governing privacy clauses such as GDPR. Designing blockchain architectures which fulfill local and global compliance rules is a complex endeavor by itself and requires careful construction, such as designated permissioned blockchains and constructed paths with auditable data pathways.

Incorporating traditional 5G systems into blockchains is technologically impractical due to prohibitive integration costs. Legacy infrastructures incur interoperability incompatibility overheads with vertical technology skilling alongside and needing robust systems in software and hardware upgrades. Systems lacking comprehensive conrolled standard frameworks expose their architecture under modular governance to intrusive conflicting security loopholes.

Last but not least, the concerns regarding energy expenditure of certain blockchain consensus approaches like Proof of Work raise questions regarding sustainability, particularly in energy-shy domains such as mobile and edge computing.These factors require the shift to more sustainable consensus algorithms such as Proof of Stake or BFT Byzantine Fault Tolerance for effective use in telecommunications networks.

In summary, the challenges presented may be addressed through thoughtful approaches, but in-depth planning combined with ground breaking ideas will be necessary.

Future Outlook and Recommendations

In light of the increased requirement for prompt, dependable, and secure exchanges of information, in 5G and future networking infrastructures, blockchain technology integration will likely be of great importance. Possible improvements of blockchain technology include the reduced latency and energy expenditure associated with mobile and edge computing systems with the lighter Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) consensus algorithms and scalable. Also, the merger of artificial intelligence (AI) with blockchain could encourage the automation of security processes through real-time adaptive threat responsiveness.

Organizations wishing to implement blockchain into their 5G infrastructures are encouraged to look into permissioned models first as they are more easily controlled than public blockchains. These also allow for better regulatory adherence, faster transactions, and overall improved efficiency. Furthermore, companies should focus on defining the boundaries of interoperability in their blockchains, as it needs to work effectively with other network protocols and outside systems. Participating in pilot projects and collaborative consortia allow testing of blockchain solutions before extensive application.

As has been articulated before, the integration of blockchain with 5G infrastructure is poised to radically change the security paradigm for emerging wireless networks. The existing security issues looming over these fast-paced systems could, in fact, be solved through the application of blockchain technology because of its decentralized trust system, nonrepudiable history, and transparency. Scalability, legal and policy constraints relevant to jurisdiction, and concerns over the application of existing systems pose significant barriers to unlocking the full potential of these innovations. Through further study, optimization of other relevant technologies, and effective execution, blockchain will emerge as the primary building block (alongside other advanced technologies) in the construction of future communications networks that demand high security and robustness.

References

1. Andrews, J. G., Buzzi, S., Choi, W., et al. (2014). “What Will 5G Be?” *IEEE Journal on Selected Areas in Communications*, 32(6), 1065–1082.
2. G.Arulkumaran J Santhosh P. Balamurugan and Velliangiri S” Secure identity key and blockchain-based authentication approach for secure data communication in multi-WSN” Concurrency and Computation: Practice and Experience,

SCI, ISSN 1532-0634, Vol.35, No.17, pp.1-24 (2023) (DOI: 10.1002/cpe.7861) (Impact Factor: 2.00) (2707-2023)

3. Zhang, Y., et al. (2020). "Security and Privacy in 5G Networks: Challenges and Solutions." IEEE Communications Surveys & Tutorials, 22(1), 396–448.
4. Mayilsamy, J., & Rangasamy, D. P. (2021). Enhanced Routing Schedule - Imbalanced Classification Algorithm for IOT based Software Defined Networks. International Academic Journal of Science and Engineering, 8(1), 01–09. https://doi.org/10.9756/IAJSE/V8I1/IAJSE0801
5. Niyato, D., et al. (2019). "A Survey on Applications of Blockchain in 5G Networks." IEEE Communications Surveys & Tutorials, 21(1), 110–132.
6. Herrera, J. A. Q., Limo, F. A. F., Tasayco-Jala, A. A., Vargas, I. M., Farias, W. B., Inga, Z. M. C., & Palacios, E. L. H. (2023). Security Issues in Internet Architecture and Protocols Based on Behavioural Biometric Block Chain-Enhanced Authentication Layer. Journal of Internet Services and Information Security, 13(3), 122-142. https://doi.org/10.58346/JISIS.2023.I3.008
7. Dorri, A., Kanhere, S. S., Jurdak, R. (2017). "Blockchain in Internet of Things: Challenges and Solutions." Computer Communications, 120, 10–29.
8. Prasanna, D. S. J. D., Punitha, K., Shrividya, G., Haval, A. M., & Vij, P. (2024). An Optimized and Cost - Effective Resource Management Model for Multi - Tier 5G Wireless Mobile Networks. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15(3), 136-149. https://doi.org/10.58346/JOWUA.2024.I3.010
9. Khan, M. A., Salah, K. (2018). "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems, 82, 395–411.
10. Udayakumar, R., Anuradha, M., Gajmal, Y. M., & Elankavi, R. (2023). Anomaly detection for internet of things security attacks based on recent optimal federated deep learning model. Journal of Internet Services and Information Security, 13(3), 104-12 1.
11. Zhang, Y., et al. (2020). "Security and Privacy in 5G Networks: Challenges and Solutions." IEEE Communications Surveys & Tutorials, 22(1), 396–448.
12. Antoniewicz, B., & Dreyfus, S. (2024). Techniques on controlling bandwidth and energy consumption for 5G and 6G wireless communication systems. International Journal of Communication and Computer Technologies, 12(2), 11-20. https://doi.org/10.31838/IJCCTS/12.02.02
13. Li, J., et al. (2019). "Security Issues of Network Functions Virtualization in 5G." IEEE Network, 33(2), 68–74.
14. Koteshwaramma, K. C., Vijay, V., Bindusree, V., Kotamraju, S. I., Spandhana, Y., Reddy, B. V. D., Charan, A. S., Pittala, C. S., & Vallabhuni, R. R. (2022). ASIC Implementation of an Effective Reversible R2B FFT for 5G Technology Using Reversible Logic. Journal of VLSI Circuits and Systems, 4(2), 5–13. https://doi.org/10.31838/jvcs/04.02.02
15. Cisco Annual Internet Report, 2018–2023.
16. Shum, A. (2024). System-level architectures and optimization of low-cost, high-dimensional MIMO antennas for 5G technologies. National Journal of Antennas and Propagation, 6(1), 58–67.
17. Khan, L. U., et al. (2020). "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions." IEEE Communications Surveys & Tutorials, 22(4), 1965–1991.
18. Ristono, A., & Budi, P. (2025). Next-gen power systems in electrical engineering. Innovative Reviews in Engineering and Science, 2(1), 34-44. https://doi.org/10.31838/INES/02.01.04
19. Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. K. (2017). "Network Slicing in 5G: Survey and Challenges." IEEE Communications Magazine, 55(5), 94–100.
20. Eiriemiokhale, K., & James, J. B. (2023). Application of the Internet of Things for Quality Service Delivery in Nigerian University Libraries. Indian Journal of Information Sources and Services, 13(1), 17–25. https://doi.org/10.51983/ijiss-2023.13.1.3463
21. Nguyen, D. C., et al. (2021). "Blockchain for 5G and Beyond Networks: A State of the Art Survey." Journal of Network and Computer Applications, 174, 102857.
22. Menaka, S. R., Gokul Raj, M., Elakiya Selvan, P., Tharani Kumar, G., & Yashika, M. (2022). A Sensor based Data Analytics for Patient Monitoring Using Data Mining. International Academic Journal of Innovative Research, 9(1), 28–36. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0905
23. Suganya E, Rajan C, 2021, An adaboost-modified classifier using particle swarm optimization and stochastic diffusion search in wireless IoT networks, Wireless Networks, 1-13.
24. Kavitha, M. (2024). Enhancing security and privacy in reconfigurable computing: Challenges and methods. SCCTS Transactions on Reconfigurable Computing, 1(1), 16 20. https://doi.org/10.31838/RCC/01.01.04
25. Peng, G., Leung, N., & Lechowicz, R. (2025). Applications of artificial intelligence for telecom signal processing. Innovative Reviews in Engineering and Science, 3(1), 26–31. https://doi.org/10.31838/INES/03.01.04
26. Bianchi, G. G., & Rossi, F. M. (2025). Reconfigurable computing platforms for bioinformatics applications. SCCTS Transactions on Reconfigurable Computing, 2(1), 16–23.
27. Hyun, K. S., Min, P. J., & Won, L. H. (2025). AI hardware accelerators: Architectures and implementation strategies. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(1), 8-19. https://doi.org/10.31838/JIVCT/02.01.02
28. Srimuang, C., Srimuang, C., & Dougmala, P. (2023). Autonomous flying drones: Agricultural supporting equipment. International Journal of Communication and Computer Technologies, 11(2), 7-12. https://doi.org/10.31838/IJCCTS/11.02.02
29. Abdul, A. M., & Nelakuditi, U. R. (2021). A New Blind Zone Free PFD in Fractional-N PLL for Bluetooth Applications. Journal of VLSI Circuits and Systems, 3(1), 19–24. https://doi.org/10.31838/jvcs/03.01.04