Internet of things and blockchain integration for security and privacy

Sumita Kumar[1,3], Amarsinh Vidhate[2]
[1]Department of Computer Engineering, Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University, Navi Mumbai, India
[2]Department of Engineering and Technology, Bharati Vidyapeeth Deemed University, Navi Mumbai, India
[3]Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University, Navi Mumbai, India

Article Info

Article history:

Received Nov 17, 2023
Revised Mar 28, 2024
Accepted Apr 17, 2024

Keywords:

Blockchain
Cloud
Internet of things
Privacy
Security

ABSTRACT

The internet of things (IoT) can be defined as a network of intelligent objects where physical objects are equipped with electronic and network components to enable connectivity. These smart objects are embedded with sensors that enable them to monitor, sense, and gather data pertaining to their surroundings, including the environment and human activities. The applications of IoT, both existing and forthcoming, show great promise in terms of enhancing convenience, efficiency, and automation in our daily lives. However, for the widespread adoption and effective implementation of the IoT, addressing concerns related to security, authentication, privacy, and recovery from potential attacks is crucial. To achieve end-to-end security in IoT environments, it is imperative to define standard framework to achieve end to end security for the IoT applications. The blockchain is distributed ledge offers advantages such as confidentiality, authenticity, and availability. In this paper, we propose a novel framework to provide security and privacy for heterogeneous IoT architecture with integration of blockchain. The framework has provided an assessment framework to deploy, govern physical deployment. The proposed framework has defined standard architecture to integrate blockchain with layered IoT architecture with customization in blockchain with lightweight cryptography and consensus mechanism to overcome integration challenges and to achieve authenticity, security, and privacy.

Corresponding Author:

Amarsinh Vidhate
Department of Engineering and Technology, Bharati Vidyapeeth Deemed University
Nerul, Navi Mumbai, Maharashtra 400706, India
Email: amar.vidhate@rait.ac.in

1. INTRODUCTION

The internet of things (IoT) represents the next phase of Internet development, revolutionizing communication and traditional applications by connecting computers and physical objects [1], [2]. This transformation leads to enhancements in productivity and service quality. The "things" in the context of IoT are any devices and objects in our surroundings with intelligence that communicate and exchange information within a vast network [3], [4]. In addition, blockchain is an immutable, timestamped, tamper-resistant, auditable, and permanent ledger of blocks designed for the storage and sharing of data in a peer-to-peer (P2P) manner. Initially, blockchain was used in cryptocurrency, recently blockchain has been applied beyond cryptocurrencies in areas such as identity management, Industry 4.0, intelligent transportation, supply chain management, and healthcare. These features include security, transactional privacy, integrity, authorization, censorship resistance, data immutability, auditability, system transparency, and fault tolerance

[1], [4]. The IoT is significantly contributing to smart city projects and driving the next industry revolution "Industry 4.0" with diverse applications in various sectors [5], [6]. Revenue generated by IoT applications across various sectors is projected to grow from $892 billion (about $2,700 per person in the US) in 2018 to an estimated $4 trillion (about $12,000 per person in the US) by 2025 [4]. IoT applications primarily focus on automating various daily tasks and enabling objects to function without human intervention. However, realizing this vision and meeting the increasing demand requires robust security measures, privacy protection, reliable authentication mechanisms, and effective safeguards against potential attacks [5]–[7].

The IoT has a large technology stack and different layers of architecture, due to such heterogeneous and dynamic nature of IoT-based intelligent environments gives rise to a unique set of authentication, privacy and security concerns and challenges at different layers of the IoT architecture [8]–[10]. IoT solutions have challenges like limited storage, computing power, networking capabilities, and power supply [8]–[10]. The fundamental security goals of traditional internet systems, namely confidentiality, integrity, authenticity, and availability along with recovery from attack must be addressed effectively and are also crucial for IoT networks. Additionally, standardized security policies and assessment frameworks for deployments are essential [11]–[13]. Existing assessments and security standards, although not specifically tailored to IoT-based smart environments [14], [15]. There are various approaches to address the IoT security and privacy challenges learning base countermeasures, encryption, fog computing, edge computing, machine learning and blockchain base approach [16]–[18].

Blockchain integration with IoT can provide the best security, authenticity, and privacy, but all these advantages come with various integration challenges like resource constraint devices, performance, high volume data, and layered IoT architecture [19]–[25]. Address security and privacy challenges for dynamic IoT architecture influenced by physical deployment demand standard framework to address unique security challenges. We have proposed a novel generic framework to deploy any IoT application. The framework expects any IoT application to analyse the environment with standard assessment framework parameters to deploy, govern, and protect. In our research, we have proposed a novel generic framework for primary security measures for heterogeneous layered IoT architecture with the integration of blockchain technology with promising security [26]–[30]. To address layered architecture integration challenges the proposed framework uses customized blockchain architecture integrated with layered IoT architecture. The proposed framework uses lightweight ECC curve cryptography for key exchange, encryption and digital signature, BLAKE2 for message digest for customized blockchain along lightweight miners with a DAG consensus mechanism.

The paper presented an overview of a novel security framework with blockchain integration. Section 2 of this paper presented an overview of the proposed assessment and IoT and blockchain in integration framework with the experimental setup. Our proposed framework addresses several challenges related to the integration of blockchain technology, paving the way for enhanced security and privacy in IoT applications. The work also discussed result analysis with different framework components in section 3.

2. METHOD

This research work aims to develop a standard security framework to ensure confidentiality, integrity, authenticity, and availability for IoT with integration with blockchain and overcome the challenges in integration. In this research work, we have presented interim details of the framework. The proposed framework for integration of IoT and blockchain has considered a layered and heterogeneous IoT environment, along with a large technology stack, challenges in blockchain integration and security framework should be generic and can apply to any IoT application. This research has considered layered IoT architecture with a physical or sensing layer, network layer, middleware layer and application. The IoT layered architecture is extended with the dew layer as an extension to the physical layer and the cloudlet layer as an extension to the middleware layer [31]–[37].

To deploy any IoT application with our proposed framework, assessment parameters will be helpful to deploy, govern, and protect IoT networks with layered functionalities and integration with blockchain to ensure security and privacy. We have proposed the standard assessment guidelines for the deployment of IoT applications with layered architecture. The assessment framework helps to ensure secure IoT deployment, and effectively manage and continuously protect heterogeneous IoT environments, which helps to define a generic security framework. The proposed assessment framework is broken down into seven key functions as following:

- Identify: any deployment must identify how to manage cyber security risk to people, systems, capabilities, assets, and data including physical environment, asset management, and information technology governance along with application requirements to configure layered IoT architecture and blockchain integration parameters for cryptography, smart contract, and data buffer.

- Categorize: any deployment must categorize the requirements based on how the system and information are processed, stored, and transmitted based on impact analysis.
- Implement: any deployment must document and implement the environment based on the above two measures.
- Protect: any deployment must document and implement appropriate security measures and blockchain integration in the environment based on the above two measures.
- Govern: any deployment must develop and implement a governance structure to understand the organization’s risk and priorities for IoT and blockchain.
- Assess: any deployment must assess the current state of implementation.
- Recover: any deployment must have a recovery plan to ensure resilience and restore to ensure availability.

The proposed generic framework for IoT layered implementation aims at achieving primary security and privacy concerns for IoT due to a heterogeneous environment with blockchain integration as shown in Figure 1. We have also considered challenges for IoT like the elimination of central authority, secure deployment of the new node, and challenges with IoT and blockchain integration like resources constraint environment, data concurrency, and high-velocity data handling for designing the layered framework. The proposed framework has been designed by considering some fundamental design principles scalability, reliability & performance, quality of service, and computational complexity.

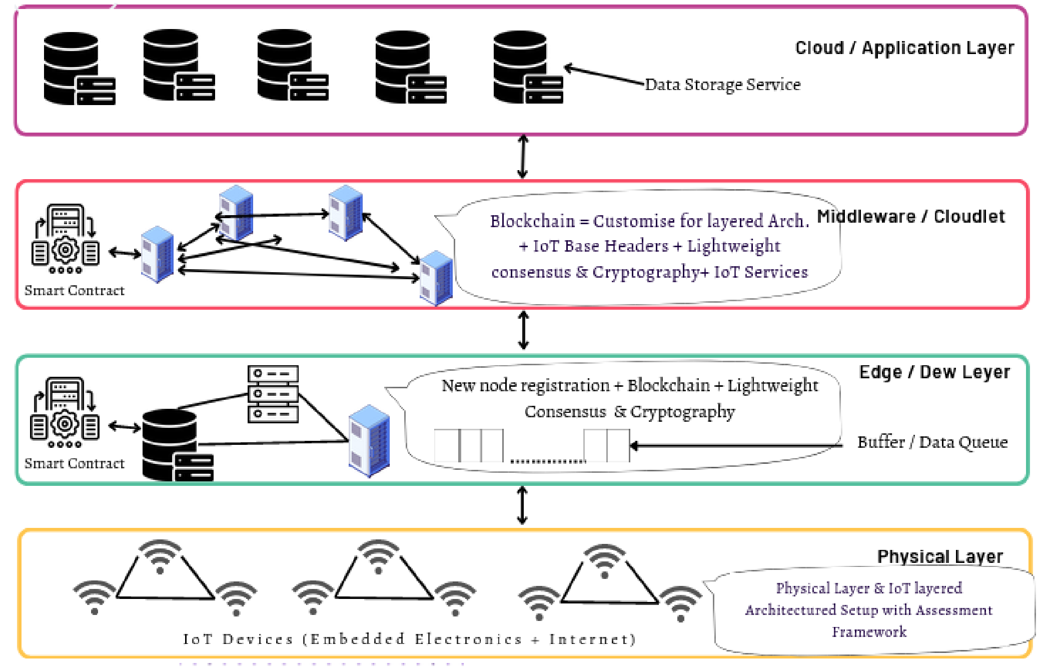

Cloud / Application Layer
Data Storage Service
Middleware / Cloudlet
Blockchain = Customise for layered Arch. + IoT Base Headers + Lightweight consensus & Cryptography+ IoT Services
Smart Contract
Edge / Dew Leyer
New node registration + Blockchain + Lightweight Consensus & Cryptography
Buffer / Data Queue
Smart Contract
Physical Layer
Physical Layer & IoT layered Architectured Setup with Assessment Framework
IoT Devices (Embedded Electronics + Internet)

Figure 1. IoT and blockchain integration layered architecture

The proposed framework has four important elements; i) secure boarding of new IoT devices and onboarding of nodes at the edge/dew layer blockchain as well as at cloudlet layer, ii) customization of blockchain at edge and middleware layer, iii) lightweight cryptographic measures, and iv) implementation of smart contract and data queue to support many real-time IoT applications. The proposed framework recommends implementing all four elements with help of various assessment parameters. The implementation of all four elements has been discussed in subsequent paragraph.

The proposed research framework configures the cloud as a data store and application interfaces responsible for analysing and processing data requested by authenticated users, things and blockchain nodes by the cloudlet layer. The cloudlet layer is configured with a fully functional blockchain. The nodes in cloudlet layers have two roles as mining nodes and blockchain participants. Each node in the cloudlet layer will be assigned reputation or stake points which is based on the success ratio of miner. The miner's node also responsible for maintaining stake for dew layer nodes. The dew layer is running with a lightweight version of the blockchain. The dew layer node also has a reputation as stake points calculated on transaction validity. The physical layer is deployed with various IoT devices registered with the IoT blockchain framework as shown in Figure 2. Both cloudlet and dew layers are configured with a direct acyclic graph (DAG) consensus mechanism, memory pool and are responsible for onboarding new nodes in the preceding layer Figure 3.

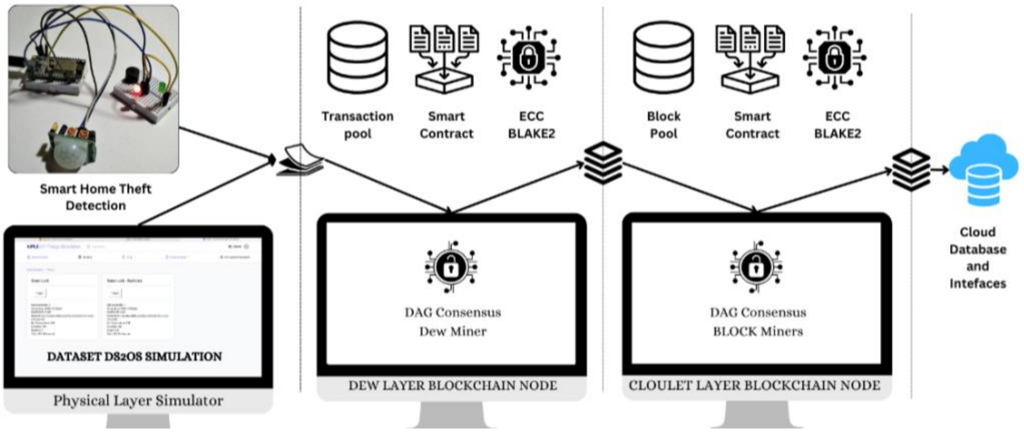


Figure 2. Experimental setup and framework components

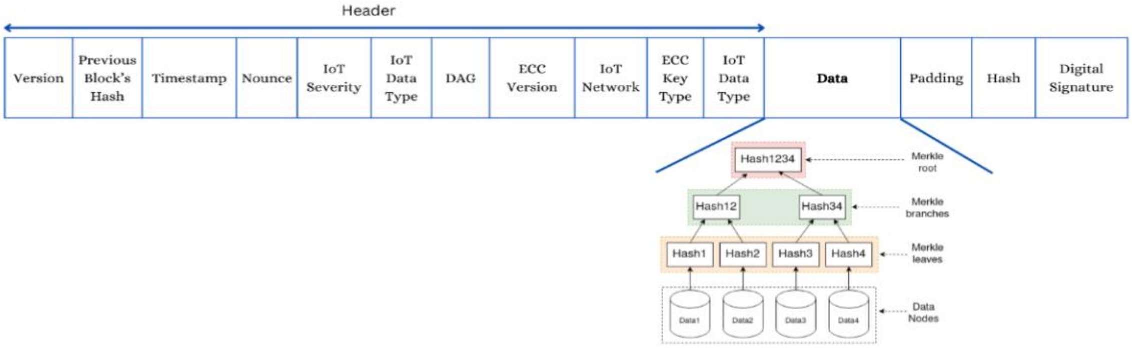


Figure 3. Blockchain block structure for IoT security framework

The experimental setup analyses the integration with real-time data as well as our ATN simulator with the DS2OS dataset. The node can work in two modes attacker and authenticate mode. We have analysed all types of records in the dataset by creating transactions with the simulator for various IoT devices and then transmitting them to the dew layer blockchain. The layer lightweight blockchain miner then validates the authenticity of the sender and transaction with the DAG consensus mechanism. A dew layer smart contract can be triggered if the transaction is critical and needs to be processed in real-time otherwise dew layer miner creates a block of transaction periodically and sends it to the cloudlet layer. The cloudlet layer miner again validates the block before proceeding with the blockchain. If the block is critical then a smart contract will be executed to support real-time IoT applications. If transactions are unauthenticated or there is an intrusion at the dew/cloudlet layer, then respective miners drop the transaction. As all communications are securely communicated, validated and stored with lightweight cryptographic measures and blockchain technology.

```
Algorithm 1: Blockchain IoT Layered Framework
Result: IoT data Security
Begin
1: If new Node at Physical Layer or Dew Layer
–   Initiate the Handshake and key Exchange with immediate upper layer blockchain.
–   Securely setup distributed elliptical curve key space for node domain p modulus, a, b, generator point g.
–   Blockchain authenticate the new node configuration transaction with DAG
```

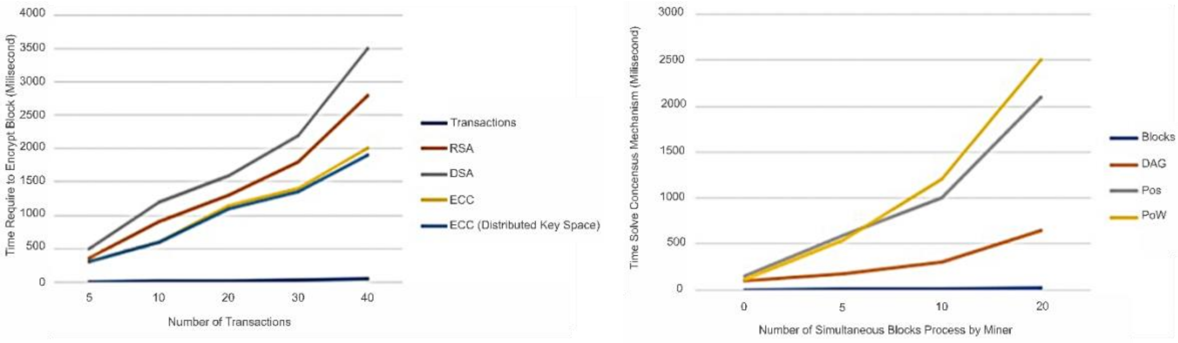
```
  –  Blockchain initiate genesis transaction for newly setup node.
2: IoT node initiate the transaction T and send to dew layer light weight blockchain
3: Dew layer blockchain miners validate the authenticity of sender and execute DAG consensus mechanism.
4: If transaction is authenticated
  –  Dew layer perform data filtration
  –  Execute the smart contract if condition meets
3: Dew layer miners periodically create blocks by creating Markle tree with encrypted transaction and
BLAK2 hash and attach ECC digital signature. Send block to cloudlet layer
4: If source is authentication is successful at cloudlet layer then.
  –  Run custom DAG consensus algorithm.
  –  Check IoT field setup in block header executes the smart contract
  –  Miner broadcast block to cloudlet layer blockchain and push actual transactions to cloud data storage
End
```

3. RESULTS AND DISCUSSION

The experimental setup has been configured with the “smart home IoT OS2 database”. The experimental setup has analysed the effectiveness of the framework with a false positive rate of the dataset. The analyse the reliability and effectiveness, this work has analysed the performance of customised blockchain with elliptic curve cryptography (ECC) algorithm with distributed key space and the effectiveness of secure onboarding of new nodes at the dew and cloudlet layer.

The challenges in IoT and blockchain integration like resources constrain environment is solves by adapted to customise lightweight blockchain with lightweight cryptographic measure and lightweight consensus mechanism. The customise blockchain with buffer pooling helps to handle high velocity data and smart helps to support real time IoT application. Our experimental setup work very effectively to maintain security and privacy for IoT applications.

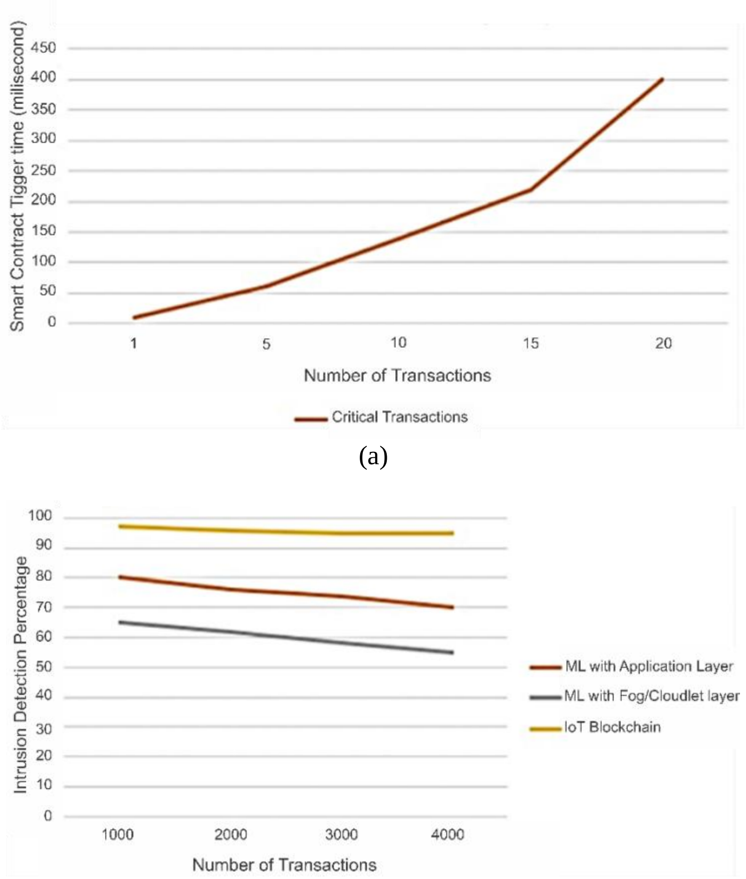
The experimental setup has analysed the time complexity of ECC vs Rivets Shamir Adelman (RSA) vs digital signature algorithm (DSA) in distributed blockchain environment. The result recorded in Figure 4(a) is include cryptographic process of IoT blockchain transaction data and parameters, represents ECC calculated value from implemented system and RSA and DSA data has been referred from respective implementation of algorithm for blockchain integration. Figure 4(b) represents DAG calculated value from implemented system and proof of stake (PoS) and proof of work (PoW) data has been referring from respective implementation of algorithm for blockchain. The DAG result seems to work much better than PoW and PoS.



(a) (b)

Figure 4. The performance ECC and DAG with proposed framework; (a) RSA Vs DSA Vs ECC Vs ECC (distributed key space), and (b) DAG Vs PoS Vs PoW

The Figure 5(a) represents comparison of time complexity for critical data block Vs smart contract trigger time for IoT blockchain mechanism to support real time IoT application. The Figure 5(b) the performance of proposed system with DS2OS intrusion detection dataset. The blockchain base IoT network perform much better, and another benefit is blockchain intrinsic characteristic of immutable database and ensure confidentiality, authenticity and availability.

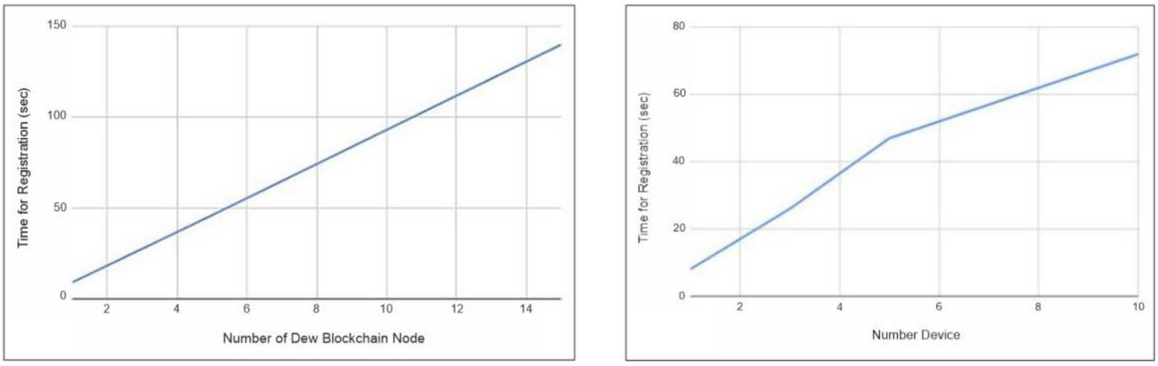


(a)

(b)

Figure 5. Performance of smart contract with framework and intrusion detection with DS2OS dataset; (a) critical transaction Vs time complexcity, and (b) DS2OS data result

The graphs in Figure 6(a) shows our analysis for registration time for device and dew layer IoT node registration time as authorize devices registration is also very important as IoT marketplace is growing very rapidly. The registration of IoT device involves handshaking between IoT device and dew layer blockchain to generate and secure sharing of secret keys for further communication. The Figure 6(b) shows performance measurement for live registration of dew layer node registration with blockchain and distributed IoT application as secure onboarding of node is necessary to keep system secure from malicious nodes.



(a)

(b)

Figure 6. Analysis performance measurement of (a) dew layer blockchain node (IoT gateway), and (b) physical layer new device registration

4. CONCLUSION

In this paper, we have presented an overview of the current state of the art of IoT, blockchain, and features of blockchain along with the integration challenges. This paper also provides an overview of As the IoT market is growing very rapidly, it is necessary to ensure primitive security measures with consideration of distributed and heterogeneous environments. Blockchain is intrinsically distributed in nature and ensures confidentiality, authenticity, and availability. This paper presented work on an assessment framework to deploy any IoT base environment and we have presented our work on a security framework with IoT and Blockchain integration. In this paper, we have proposed a customized blockchain for IoT-based environments and our experimental setup with analysis.

REFERNCES

[1] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, pp. 32–37, Feb. 2017, doi: 10.1109/I-SMAC.2017.8058363.

[2] M. Yuvaraju, S. Kumar, K. Singh, G. N. Rao, B. J. Kumar, and K. Vigneshwaran, "Transformer monitoring and security system using IoT," in *IDCIoT 2023 - International Conference on Intelligent Data Communication Technologies and Internet of Things, Proceedings*, pp. 84–89, Jan. 2023, doi: 10.1109/IDCIoT56793.2023.10053405.

[3] S. Kumar and A. Vidhate, "Issues and future trends in IoT security using blockchain: a review," in *IDCIoT 2023 - International Conference on Intelligent Data Communication Technologies and Internet of Things, Proceedings*, pp. 976–984, Jan. 2023, doi: 10.1109/IDCIoT56793.2023.10053430.

[4] S. Rathore, J. H. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," *IEEE Access*, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[5] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018, doi: 10.1109/ACCESS.2018.2863244.

[6] C. S. Park and H. M. Nam, "Security architecture and protocols for secure MQTT-SN," *IEEE Access*, vol. 8, pp. 226422–226436, 2020, doi: 10.1109/ACCESS.2020.3045441.

[7] D. Shin, K. Yun, J. Kim, P. V. Astillo, J.-N. Kim, and I. You, "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019, doi: 10.1109/ACCESS.2019.2943929.

[8] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020, doi: 10.1109/ACCESS.2020.3006358.

[9] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," *Computer Science Review*, vol. 50, Nov. 2023, doi: 10.1016/j.cosrev.2023.100585.

[10] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," *IEEE Access*, vol. 8, pp. 88892–88932, 2020, doi: 10.1109/ACCESS.2020.2993553.

[11] C. Choi and J. Choi, "Ontology-based security context reasoning for power IoT-cloud security service," *IEEE Access*, vol. 7, pp. 110510–110517, 2019, doi: 10.1109/ACCESS.2019.2933859.

[12] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A review of security standards and frameworks for IoT-based smart environments," *IEEE Access*, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[13] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[14] S. Kumar *et al.*, "An optimized intelligent computational security model for interconnected blockchain-IoT system & cities," *Ad Hoc Networks*, vol. 151, Dec. 2023, doi: 10.1016/j.adhoc.2023.103299.

[15] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Networks*, vol. 152, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.

[16] V. Varriale, A. Cammarano, F. Michelino, and M. Caputo, "Integrating blockchain, RFID and IoT within a cheese supply chain: A cost analysis," *Journal of Industrial Information Integration*, vol. 34, Aug. 2023, doi: 10.1016/j.jii.2023.100486.

[17] S. Siboni *et al.*, "Security testbed for internet-of-things devices," *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23–44, Mar. 2019, doi: 10.1109/TR.2018.2864536.

[18] M. G. Samaila, J. B. F. Sequeiros, T. Simoes, M. M. Freire, and P. R. M. Inacio, "IoT-HarPSecA: A framework and roadmap for secure design and development of devices and applications in the IoT space," *IEEE Access*, vol. 8, pp. 16462–16494, 2020, doi: 10.1109/ACCESS.2020.2965925.

[19] S. Zaman *et al.*, "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey," *IEEE Access*, vol. 9, pp. 94668–94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[20] K. S. S. Bajpai, "Survey on blockchain technology in IoT for security," *Engineering and Technology Journal for Research and Innovation (ETJRI)*, vol. 3, no. 2, pp. 5-11, Jul. 2021.

[21] S. N. Swamy and S. R. Kota, "An empirical study on system level aspects of internet of things (IoT)," *IEEE Access*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[22] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-internet of things (M-IoT): A survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020, doi: 10.1109/ACCESS.2020.3022661.

[23] S. Khanam, I. B. Ahmedy, M. Y. I. Idris, M. H. Jaward, and A. Q. B. M. Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020, doi: 10.1109/ACCESS.2020.3037359.

[24] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure," *IEEE Access*, vol. 9, pp. 71856–71867, 2021, doi: 10.1109/ACCESS.2021.3079312.

[25] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[26] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A Survey on the Integration of Blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[27] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019, doi: 10.1109/ACCESS.2019.2913682.

[28] M. Muneeb, Z. Raza, I. U. Haq, and O. Shafiq, "SmartCon: a blockchain-based framework for smart contracts and transaction management," *IEEE Access*, vol. 10, pp. 10719–10730, 2022, doi: 10.1109/ACCESS.2021.3135562.

[29] N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018, doi: 10.1016/j.procs.2018.05.140.

[30] A. E. S. Leni, R. Shankar, R. Thiagarajan, and V. R. Patil, “Block-chain based secure data access over internet of health application things (IHoT),” *KSII Transactions on Internet and Information Systems*, vol. 17, no. 5, pp. 1484–1502, May 2023, doi: 10.3837/tiis.2023.05.010.

[31] S. Singh, A. S. M. S. Hosen, and B. Yoon, “Blockchain security attacks, challenges, and solutions for the future distributed IoT network,” *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[32] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, “Secure intelligent fuzzy blockchain framework: effective threat detection in IoT networks,” *Computers in Industry*, vol. 144, Jan. 2023, doi: 10.1016/j.compind.2022.103801.

[33] J. Wang, W. Yi, M. Yang, J. Ma, S. Zhang, and S. Hao, “Enhance the trust between IoT devices, mobile apps, and the cloud based on blockchain,” *Journal of Network and Computer Applications*, vol. 218, Sep. 2023, doi: 10.1016/j.jnca.2023.103718.

[34] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, “A survey on role of blockchain for IoT: applications and technical aspects,” *Computer Networks*, vol. 227, May 2023, doi: 10.1016/j.comnet.2023.109726.

[35] S. Shreya, K. Chatterjee, and A. Singh, “BFSF: A secure IoT based framework for smart farming using blockchain,” *Sustainable Computing: Informatics and Systems*, vol. 40, 2023, doi: 10.1016/j.suscom.2023.100917.

[36] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, “Survey on blockchain-based smart contracts: technical aspects and future research,” *IEEE Access*, vol. 9, pp. 87643–87662, 2021, doi: 10.1109/ACCESS.2021.3068178.

[37] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, “Recent advances in smart contracts: a technical overview and state of the art,” *IEEE Access*, vol. 8, pp. 117782–117801, 2020, doi: 10.1109/ACCESS.2020.3005020.

BIOGRAPHIES OF AUTHORS

Sumita Kumar is working as an Assistant Professor at Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, in the Department of Computer Science Engineering. Her academic qualification is Ph.D. pursuing in (Computer Engineering) from Dr. D.Y. Patil University Nerul Navi Mumbai, M.Tech. (Computer Engineering) from Bharati Vidyapeeth Deemed University Pune, and B.E. (Computer Science & Engineering). She is in the teaching profession for more than 7 years. Her main area of interest includes machine learning, network security, IoT, blockchain, cryptography, and cyber security. She can be contacted at email: sumitakumar02@gmail.com.

Amarsinh Vidhate is working as a professor for the last 8 years, in the Department of Computer Engineering at RAIT, D. Y. Patil deemed to be university. He has 26+ years of academic experience and almost 80+ national and international research papers, published at international conferences and referred journals. His areas of research are protocol stacks, computer networking & security, VaNET, IoT, and 5G applications especially healthcare applications with AI & ML. He is a PG guide and Ph.D. guide at the University of Mumbai, as well as D.Y. Patil University. His special interest is in mass education and designing content that is useful for the masses to make them employable. He is a member of professional bodies like IEEE, CSI, and ISTE. He can be contacted at email: amar.vidhate@rait.ac.in.