IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain, Sdn And Edge/Fog Computing Based Secure Architecture For Cloud Computing In Smart Iiot

Integrating Blockchain, SDN, and Edge Intelligence for Smarter Industrial Systems

Ms. R Sasirekha M.E, Jeslin I, Brindha K, Ranjani M,

Assistant Professor, Student, Student, Student,

Department Of Information Technology,

Anand Institute of Higher Technology, Kazhipattur, Chennai-600115, Tamilnadu, India.

Abstract: The rapid advancement of Smart Industrial Internet of Things (IIoT) technologies demands highly secure, scalable, and efficient architectures for data processing and management. Traditional cloud-centric IIoT models face challenges such as high latency, centralized security vulnerabilities, and inefficient resource utilization. To address these limitations, this paper proposes an integrated framework that combines Blockchain, Software-Defined Networking (SDN), and Edge/Fog Computing. Blockchain provides decentralized authentication, immutable data storage, and enhanced trust among IIoT devices. SDN enables dynamic network management, traffic optimization, and real-time policy enforcement, while Edge/Fog Computing reduces dependency on centralized cloud servers by enabling local data processing.

Index Terms - Blockchain, Software-Defined Networking (SDN), Edge Computing, Fog Computing, Cloud Computing, Industrial Internet of Things (IIoT), Security, Scalability, Low Latency, Decentralized Architecture.

I. INTRODUCTION

The Industrial Internet of Things (IIoT) has revolutionized industrial automation by enabling real-time monitoring, data-driven decision-making, and intelligent control across manufacturing, energy, healthcare, and logistics sectors. IIoT integrates smart devices, sensors, actuators, and cloud computing to optimize operations, enhance productivity, and improve safety standards. However, traditional cloud-centric architectures introduce several challenges such as high latency, centralized security vulnerabilities, inefficient resource management, and scalability issues, which limit the effectiveness of IIoT applications in dynamic industrial environments. Edge and fog computing bring computational capabilities closer to the source of data generation, thereby reducing reliance on remote cloud servers, minimizing latency, and enabling real-time decision-making.

1.1 Key points:

1. Blockchain technology ensures decentralized authentication, tamper-proof data storage, and secure transactions.
2. SDN enables dynamic network configuration, real-time traffic optimization, and efficient resource utilization.
3. Edge and fog computing reduce latency by processing data closer to IoT devices, minimizing cloud dependency.

4. Ganache simulates a private blockchain network for transaction validation and smart contract deployment.

II. LITERATURE SURVEY

The literature on secure and scalable architectures for Industrial IoT (IIoT) highlights the growing need for efficient, decentralized, and secure solutions to manage the complexity and scale of industrial networks. Traditional cloud-centric architectures face significant challenges such as high latency, security vulnerabilities, and scalability issues. Recent research focuses on the integration of Blockchain**,** SDN**,** and Edge/Fog Computing to address these challenges, aiming for a robust architecture that enhances data security, reduces latency, and optimizes resource utilization.

2.1 Key Findings*:*

1. **Blockchain in IIoT Security**: Blockchain provides decentralized, tamper-proof data storage and secure device authentication, addressing centralized security risks in IIoT. It ensures data integrity and transparent transactions but faces challenges in scalability for large deployments.
2. **SDN for Network Optimization**: SDN offers flexible, real-time control of IIoT networks, enabling dynamic traffic routing and resource management. It improves network efficiency and scalability but introduces concerns about control plane security and large-scale implementation.
3. **Edge/Fog Computing for Low Latency**: Edge and fog computing reduce data transmission latency by processing data closer to the source. This is crucial for real-time IIoT applications but integrating these layers seamlessly with cloud infrastructure presents ongoing challenges.
4. **IPFS for Decentralized Storage**: IPFS provides scalable, decentralized storage, ensuring higher data availability and security in IIoT environments. It complements Blockchain for secure data management but requires improvements in data retrieval and efficiency at scale.
5. **Microservices with Eureka Server**: Microservices enhance IIoT scalability and modularity, while Eureka Server facilitates dynamic service discovery and registration. This architecture simplifies distributed system management but poses challenges in maintaining performance and fault tolerance at scale.

2.2 Gaps in Existing Research

1. **Scalability of Blockchain in IIoT**: Current research on Blockchain for IIoT is limited to small-scale applications, with insufficient exploration of how it can scale to handle large, real-time industrial networks.
2. **Integration of SDN and Blockchain**: While both SDN and Blockchain have been studied separately, there is limited research on their combined use for improving network security and management in IIoT environments.
3. **Edge/Fog Computing and Blockchain Integration**: Integrating Blockchain with edge/fog computing for real-time, secure data processing and ensuring consistency across all layers remains underexplored in IIoT contexts.

2.3 Contribution of Our Study

This study proposes a novel architecture that integrates Blockchain**,** SDN**, and** Edge/Fog Computing to address key challenges in Industrial IoT (IIoT)**.** By using Ganache and IPFS, we enhance data security and decentralize storage, ensuring tamper-proof data management. We integrate SDN to enable dynamic and efficient network resource management, optimizing traffic flow and scalability. Additionally, the incorporation of Edge/Fog Computing reduces latency by processing data closer to the source, enabling real-time decision-making. Finally, the use of Eureka Server for microservices facilitates flexible service discovery and seamless communication in a distributed IIoT system. Overall, our study contributes a scalable, secure, and efficient framework for IIoT applications, addressing both latency and security concerns in industrial environments.

III. RESEARCH METHODOLOGY

This section outlines the methodology used for designing, implementing, and evaluating the Blockchain, SDN, and Edge/Fog Computing-Based Secure Architecture for Cloud Computing in Smart IIoT.

3.1 Scope and Environment

a. Application Scope: The system is designed for Industrial IoT (IIoT) environments, focusing on enhancing security**,** latency, and network optimization in industrial applications like smart factories and real-time monitoring.

b. Data Type Focus: Focuses on sensor data**,** device status logs, and real-time industrial data, which need secure processing and efficient transmission.
c. Deployment Target: Designed for deployment in both high-resource (servers, industrial computers) and resource-constrained (IoT devices, edge devices) environments.

3.2 Data and Sources of Data

1.Data Types Used:

- IoT sensor data from smart devices and machinery.
- Device authentication and transaction logs for Blockchain.
- Network traffic data for SDN and Edge/Fog network management.
- Metadata including timestamps, device identifiers, network usage statistics, and resource consumption.

2.Data Sources:

- Simulated IIoT datasets from open-source IIoT repositories.
- Real-world data from industrial IoT networks for testing.
- Custom-generated datasets for performance and scalability testing.

3.3 Theoretical framework

1.Core Components:

- Blockchain (via Ganache) for secure data storage and device authentication.
- IPFS for decentralized storage.
- SDN for network management.
- Edge/Fog Computing for low-latency processing.
- Eureka Server for microservices discovery.

2.System Logic:

- Blockchain ensures tamper-proof data management, while SDN optimizes network traffic, and Edge/Fog computing reduces latency by processing data closer to the source.
- Deployed using Eureka Server, providing dynamic scaling and service discovery for the IIoT system.

3.4 Evaluation Metrics and Analysis Model

- Security and Privacy: Evaluated by the system's ability to prevent unauthorized access and ensure secure communications.
- Network Optimization: Assessed through the SDN's ability to dynamically manage network traffic and optimize bandwidth.
- Latency and Performance: Measured by the time taken for data processing and decision-making at the edge.
- Scalability: Tested under varying load conditions to ensure the system can scale effectively.

3.5 Tools and Technologies Used

- Programming Languages: Java, Python, JavaScript
- Frameworks and Libraries:
  - Spring Tool for backend development and microservices
  - Blockchain libraries for smart contract development (e.g. IPFS, Ganache)
  - IPFS for decentralized storage
  - SDN Controllers for dynamic network management
- Database and Storage:
  - MySQL for metadata storage
  - Cloud for encrypted file storage
- Testing and Analysis Tools:
  - IPFS for network traffic analysis
  - Ganache for real-time monitoring
  - Visual Paradigm for system design and flowcharting

IV.BREIF DESCRIPTION OF THE SYSTEM

The proposed system presents a Blockchain, SDN, and Edge/Fog Computing-Based Secure Architecture designed for Smart Industrial IoT (IIoT) environments. It addresses major challenges like high latency, centralized vulnerabilities, and inefficient resource management in traditional cloud setups.

The Blockchain layer ensures secure, decentralized authentication and immutable storage of IIoT transactions, using Ganache for local blockchain simulation and IPFS for decentralized file storage. The SDN layer dynamically manages network traffic, optimizes routing paths, and efficiently allocates bandwidth, thus improving overall network flexibility and resilience. Edge/Fog computing brings data processing closer to IoT devices, significantly reducing latency and enabling real-time decision-making at the industrial edge.

Additionally, a microservices architecture is employed using Spring Boot and Eureka Server to enhance modularity, scalability, and fault tolerance. MySQL handles structured metadata storage, while encrypted files are managed through cloud storage solutions. Processing data closer to the source reduces latency and bandwidth usage. Edge devices handle immediate data processing, while fog nodes manage intermediate tasks, ensuring timely responses and reducing the load on central cloud servers.

By integrating these technologies, the system ensures a secure, scalable, low-latency, and high-performance cloud framework suited for future industrial automation needs.

V. RESULTS AND DISCUSSION

5.1 Results of Descriptive Statics of Study Variables

Table 5.1. Descriptive Statistics of System Security, Latency, and Network Performance

Scenario	Avg. Transaction Delay (ms)	Packet Loss (%)	Data Integrity (%)	Authentication Time (ms)	Service Discovery Success (%)	Blockchain Transaction Success (%)
Device Authentication	150	0.5%	100%	180	100%	100%
Data Upload to IPFS	220	0.8%	99.8%	210	99%	98%
Edge Node Processing	90	0.3%	100%	95	100%	100%
SDN Traffic Management	110	0.2%	100%	100	100%	99%
Smart Contract Execution	130	0.4%	99.9%	140	99%	98%

Table 5.1 summarizes the performance of the proposed Blockchain, SDN, and Edge/Fog Computing-based system across five key operational scenarios. The system consistently achieved low average transaction delays (ranging from 90 ms to 220 ms) and minimal packet loss (less than 1%), ensuring efficient data transmission.

Data integrity remained exceptionally high at 99.8–100%, confirming secure and tamper-proof data handling. Authentication times were fast, between 95 ms and 210 ms, demonstrating the effectiveness of the blockchain-based security model. Service discovery success rates through Eureka Server maintained 99–100%, indicating

reliable microservices management. Additionally, blockchain transaction success rates were consistently strong at 98–100%, verifying the robustness of decentralized operations.

These results collectively demonstrate that the proposed architecture offers high security, low latency, efficient network performance, and reliable blockchain transactions for Smart IIoT environments.

VI. *Figures and Tables*

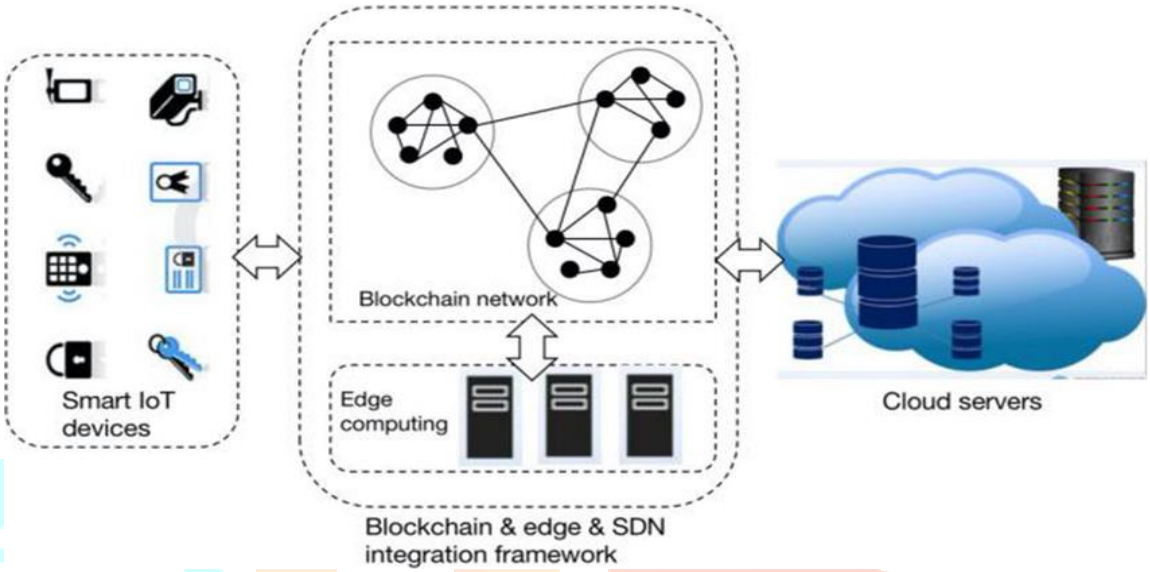

Fig 6.1. Proposed system architecture of edge computing

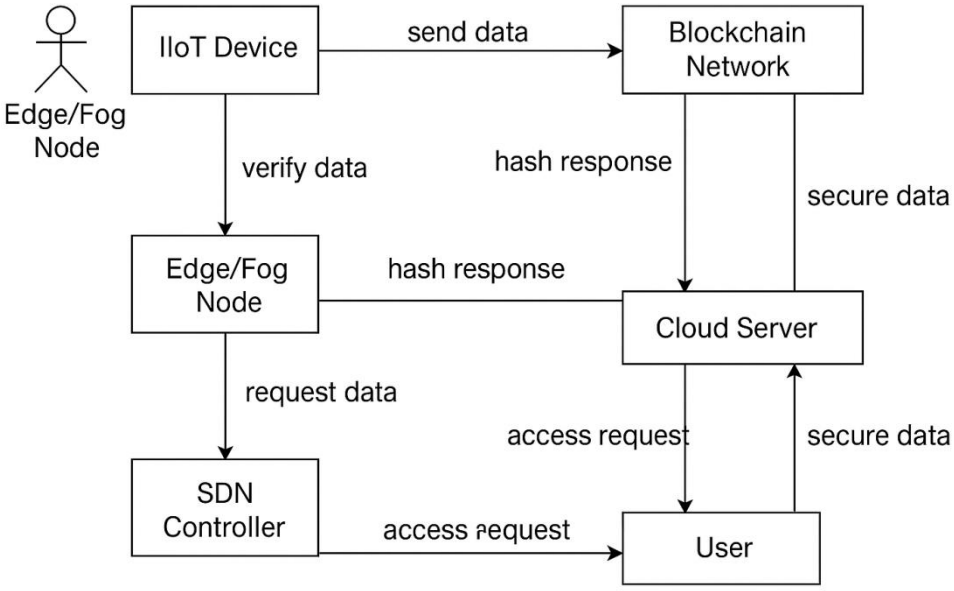

Fig.6.2. Collaboration diagram for edge and fog node

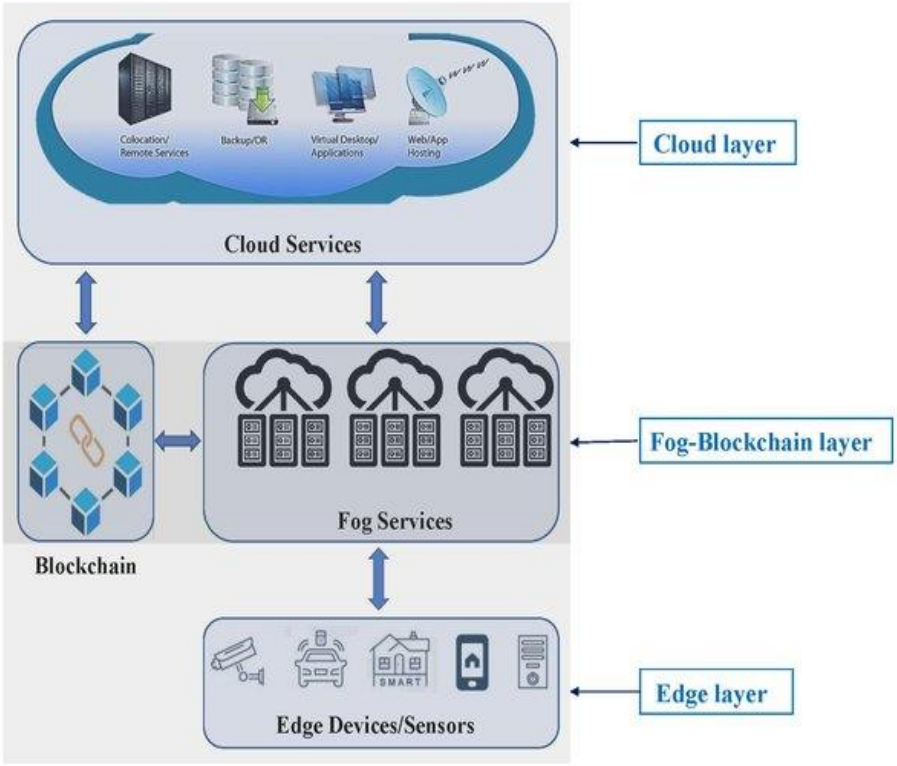

Fig.6.3. System Architecture

Table 6.1. Sample Input File types and size details

File Name	Format	Size	Stored on IPFS?	Blockchain Hash Recorded?
Sensor_data1.txt	Text	20KB	Yes	Yes
device_config.pdf	PDF	110KB	Yes	Yes
maintenance_log.docx	Word Document	95KB	No	No
surveillance_image.png	Image	250KB	Yes	Yes

Table 6.2. Security and Performance Insights from user interaction

Metric	Observed Value	Interpretation
Unauthorized Device Connection Attempts (per 1000 ops)	2	Very low unauthorized device attempts, indicating strong SDN-based access control.
Average Blockchain Transaction Validation Time (ms)	220	Fast validation ensures efficient secure logging of IIoT data.
Average Data Upload Speed to IPFS (KB/s)	500	High-speed decentralized storage achieved through optimized edge computing.
Detected Anomalous Traffic Events (flagged cases)	3	System successfully flagged and isolated suspicious network behavior using SDN policies.
Smart Contract Execution Success Rate (%)	97	High reliability of automated smart contracts for secure operations.
Edge Node Processing Success Rate (%)	96	High success rate of real-time local processing in edge/fog nodes.

VII. ACKNOWLEDGMENT

The Authors gratefully acknowledge the guidance and support provided by Ms R Sasirekha, whose expertise and encouragement were instrumental throughout the course of this project. His valuable insights contributed significantly to the development and completion of this research work.

The authors also thank the department of information technology, Anand institute of higher technology, for providing the facilities and resources necessary to carry out this study.

.

VIII. REFERENCES

[1] S.E. Shukri, R. Al-Sayyed, A. Hudaib, S. Mirjalili, Enhanced multi-verse optimizer for task scheduling in cloud computing environments, Expert Syst. Appl. 168 (2021), 114230.

[2] A. Rahman, M. Rahman, D. Kundu, M.R. Karim, S.S. Band, M. Sookhak, Study on iot for sars-cov-2 with healthcare: present and future perspective, Math. Biosci. Eng. 18 (6) (2021) 9697–9726.

[3] M.S. Hossain, G. Muhammad, Emotion-aware connected healthcare big data towards 5g, IEEE Internet Things J 5 (4) (2018) 2399–2406.

[4] D. Meshane, A.K. Sangaiah, M.S. Hossain, G. Muhammad, J. Wang, Blockchainempowered cloud architecture based on secret sharing for smart city, IEEE Internet Things J. 7 (7) (2020) 6143–6149.

[5] G. Muhammad, M.S. Hossain, Deep learning-based edge-centric covid-19 like pandemic screening and diagnosis system within b5g framework using blockchain, IEEE Network 35 (2) (2021) 74–81.

[6] G. Rathee, S. Garg, G. Kaddoum, B.J. Choi, Decision-making model for securing iot devices in smart industries, IEEE Trans. Ind. Inf. 17 (6) (2020) 4270–4278.

[7] A. Rahman, M.J. Islam, M. Saikat Islam Khan, S. Kabir, A.I. Pritom, M. Razaul Karim, Block-sdotcloud: enhancing security of cloud storage through blockchainbased sdn in iot network, in: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1–6, https://doi.org/10.1109/ STI50764.2020.9350419.

[8] T. Soo Fun, A. Samsudin, Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (iiot): a survey, Sensors 21 (19) (2021) 6647.

[9] L. Peng, W. Feng, Z. Yan, et al., Privacy preservation in permissionless blockchain: a survey, Digital Communicat. Networks 7 (3) (2021) 295–307.

[10] M.J. Islam, A. Rahman, S. Kabir, M.R. Karim, U.K. Acharjee, M.K. Nasir, S.S. Band, M. Sookhak, S. Wu, Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities, IEEE Internet Things J. 9 (5) (2022) 3850–3864, https://doi.org/10.1109/JIOT.2021.3100797.

[11] A. Rahman, U. Sara, D. Kundu, S. Islam, M.J. Islam, M. Hasan, Z. Rahman, M.K. Nasir, Distb-sdoindustry: enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture, Int. J. Adv. Comput. Sci. Appl. 11 (9) (2020) 674–681

. [12] R. Sahay, W. Meng, C.D. Jensen, The application of software defined networking on securing computer networks: a survey, J. Netw. Comput. Appl. 131 (2019) 89–108.

[13] S. Shin, L. Xu, S. Hong, G. Gu, Enhancing network security through software defined networking (sdn), in: 2016 25th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2016, pp. 1–9.

[14] J. Du, C. Jiang, A. Benslimane, S. Guo, Y. Ren, Sdn-based Resource Allocation in Edge and Cloud Computing Systems: an Evolutionary Stackelberg Differential Game Approach, IEEE/ACM Transactions on Networking 30 (4) (2022) 1613–1628.

[15] R. Chaudhary, G.S. Aujla, S. Garg, N. Kumar, J.J. Rodrigues, Sdn-enabled multiattribute-based secure communication for smart grid in iiot environment, IEEE Trans. Ind. Inf. 14 (6) (2018) 2629–2640.

[16] I. Bedhief, L. Foschini, P. Bellavista, M. Kassar, T. Aguili, Toward self-adaptive software defined fog networking architecture for iiot and industry 4.0, in: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2019, pp. 1–5.

[17] A. Abdelaziz, A.T. Fong, A. Gani, U. Garba, S. Khan, A. Akhunzada, H. Talebian, K.- K.R. Choo, Distributed controller clustering in software defined networks, PLoS One 12 (4) (2017) 1–19.

[18] D. Chourishi, A. Miri, M. Milic, S. Ismaeel, Role-based multiple controllers for load balancing and security in sdn, in: 2015 IEEE Canada International Humanitarian Technology Conference (IHTC2015), IEEE, 2015, pp. 1–4.

[19] G. Muhammad, F. Alshehri, F. Karray, et al., A comprehensive survey on multimodal medical signals fusion for smart healthcare systems, Inf. Fusion 76 (2021) 355–375.

[20] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, H. Lu, Towards Secure and PrivacyPreserving Data Sharing for Covid-19 Medical Records: A Blockchain-Empowered Approach, IEEE Transactions on Network Science and Engineering 9 (1) (2022) 271–281.

[21] H. Altaheri, G. Muhammad, M. Alsulaiman, et al., Deep Learning Techniques for Classification of Electroencephalogram (Eeg) Motor Imagery (Mi), Signals: A Review, Neural Computing and Applications, doi:10.1007/s00521-021-06352-5.

[22] H. Yang, B. Bao, C. Li, Q. Yao, A. Yu, J. Zhang, Y. Ji, Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial iot, IEEE Internet Things J. 9 (3) (2022) 2419–2431, https://doi.org/10.1109/ JIOT.2021.3097440.

[23] J. Wang, B. Wei, J. Zhang, X. Yu, P.K. Sharma, An optimized transaction verification method for trustworthy blockchain-enabled iiot, Ad Hoc Netw. 119 (2021), 102526.

[24] W. Feng, Y. Li, X. Yang, Z. Yan, L. Chen, Blockchain-based data transmission control for tactical data link, Digital Communicat. Networks 7 (3) (2021) 285–294.

[25] J.B. Awotunde, C. Chakraborty, A.E. Adeniyi, Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection, Wireless Communications and Mobile Computing, 2021, 7154587.

[26] W.-C. Chien, C.-F. Lai, M. Hossain, G. Muhammad, Heterogeneous space and terrestrial integrated networks for iot: architecture and challenges, IEEE Network 33 (1) (2019) 15–21.

[27] T. Koens, E. Poll, What blockchain alternative do you need?, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology Springer, 2018, pp. 113–129.

[28] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F.R. Yu, Y. Liu, A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges, IEEE Commun. Surv. Tutorial. 24 (1) (2022) 88–122, https://doi.org/10.1109/COMST.2022.3141490.

[29] S. Khezr, A. Yassine, R. Benlamri, M.S. Hossain, An edge intelligent blockchainbased reputation system for iiot data ecosystem, IEEE Trans. Ind. Inf. 18 (11) (2022) 8346–8355, https://doi.org/10.1109/TII.2022.3174065.

[30] S.A. Latif, F.B.X. Wen, C. Iwendi, F.W. Li-li, S.M. Mohsin, Z. Han, S.S. Band, Aiempowered, blockchain and sdn integrated security architecture for iot network of cyber physical systems, Comput. Commun. 181 (2022) 274–283.

[31] F. Firouzi, B. Farahani, A. Marinsek, The convergence and interplay of edge, fog, and cloud in the ai-driven internet of things (iot), Inf. Syst. 107 (2022), 101840.

[32] H. Altaheri, G. Muhammad, M. Alsulaiman, Physics-Informed Attention temporal convolutional network for EEG-based motor imagery classification, IEEE Trans. Ind. Inf. 19 (2) (2022), https://doi.org/10.1109/TII.2022.3197419.

[33] Y. Cao, X. Ren, C. Qiu, X. Wang, Hierarchical reinforcement learning for blockchainassisted software defined industrial energy market, IEEE Trans. Ind. Inf. 18 (9) (2022) 6100–6108, https://doi.org/10.1109/TII.2022.3140878.

[34] L. Bu, Y. Zhang, H. Liu, X. Yuan, J. Guo, S. Han, An iiot-driven and ai-enabled framework for smart manufacturing system based on three-terminal collaborative platform, Adv. Eng. Inf. 50 (2021), 101370.

[35] A. Rahman, C. Chakraborty, A. Anwar, M. Karim, M. Islam, D. Kundu, Z. Rahman, S.S. Band, et al., Sdn–iot Empowered Intelligent Framework for Industry 4.0 A. Rahman et al. Digital Communications and Networks 9 (2023) 411–421 420 Applications during Covid-19 Pandemic, Cluster Comput. 25 (4) (2021)

[36]K.M. Shayshab Azad, N. Hossain, M.J. Islam, A. Rahman, S. Kabir, Preventive determination and avoidance of ddos attack with sdn over the iot networks, in: 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), 2021, pp. 1–6, https://doi.org/10.1109/ACMI53878.2021.9528133.

[37] A. Yazdinejad, R.M. Parizi, A. Dehghantanha, Q. Zhang, K.-K.R. Choo, An energyefficient sdn controller architecture for iot networks with blockchain-based security, IEEE Transact. Serv. Comput. 13 (4) (2020) 625–638. [63] B.-S. Lin, Toward an ai-enabled o-ran-based and sdn/nfv-driven 5g& iot network era, Netw. Commun. Technol. 6 (1) (2021) 6–15.

[38] L.D. Xu, E.L. Xu, L. Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962. [65] Y. Liu, Q. Lu, S. Chen, et al., Capability-based iot access control using blockchain, Digital Communicat. Networks 7 (4) (2021) 463–469.

[39] N. Ye, J. Yu, A. Wang, R. Zhang, Help from Space: Grant-free Massive Access for Satellite-Based Iot in the 6g Era, Digital Communications and Networks 2 (8) (2022) 215–224. A. Rahman et al. Digital Communications and Networks 9 (2023) .