

WWJMRD 2025; 11(04): 45-50 www.wwjmrd.com International Journal Peer Reviewed Journal Refereed Journal Indexed Journal Impact Factor SJIF 2017: 5.182 2018: 5.51, (ISI) 2020-2021: 1.361 E-ISSN: 2454-6615

#### Sudip Chakraborty

D.Sc. Researcher, Institute of Computer Science and Information Sciences, Srinivas University, Mangalore, India.

#### **Deep Chakraborty**

MCKV Institute of Engineering, Howrah, West Bengal, India.

Correspondence: Sudip Chakraborty

D.Sc. Researcher, Institute of Computer Science and Information Sciences, Srinivas University, Mangalore, India.

# Decentralized Remote Switch Operation for Industrial Safety via Blockchain

## Sudip Chakraborty, Deep Chakraborty

#### Abstract

In modern industrial environments, ensuring the safety and efficiency of electrical systems is paramount. Traditional remote switch operations often rely on centralized control systems that are prone to single points of failure, cyber-attacks, and limited transparency. This paper proposes a novel decentralized approach to remote switch operation for industrial safety using blockchain technology. By leveraging the immutable, transparent, and tamper-resistant nature of blockchain, the proposed system enables secure and verifiable control of industrial switches, eliminating the need for centralized authority.

The architecture integrates smart contracts deployed on a blockchain network to automate switch control logic, access permissions, and event logging. Each switch operation—whether initiated by human operators or IoT-based sensors is recorded on the blockchain, ensuring traceability and accountability. The system also incorporates consensus mechanisms to validate actions, preventing unauthorized access or malicious activities. To enhance responsiveness and real-time control, a lightweight node framework is implemented at the edge level, interfacing with industrial equipment.

The proposed solution was tested in a simulated industrial setup, demonstrating improved reliability, fault tolerance, and security over conventional methods. Key performance indicators, including latency, operational accuracy, and network resilience, were analyzed, revealing that blockchain integration does not significantly compromise real-time responsiveness while significantly improving system integrity and auditability.

This research highlights the potential of decentralized technologies in enhancing industrial safety systems and opens avenues for future work in integrating AI-driven analytics and cross-industry blockchain interoperability.

**Keywords:** Blockchain, Decentralized Control, Remote Switch Operation, Industrial Safety, Smart Contracts, IoT, Edge Computing, Cybersecurity, Fault Tolerance, Real-time Monitoring.

#### 1. Introduction

In industrial environments, the operation of electrical switches plays a critical role in managing power distribution, machinery control, and ensuring worker safety. Traditionally, these systems have been governed by centralized control architectures, which are not only susceptible to single points of failure but also vulnerable to cyberattacks, system malfunctions, and human errors. As industrial automation becomes more complex and geographically distributed, the need for secure, transparent, and tamper-proof control mechanisms is becoming increasingly urgent. This paper examines a blockchain-based, decentralized approach to remote switch operation, aiming to enhance industrial safety and operational reliability.

The evolution of Industry 4.0 has brought with it a convergence of cyber-physical systems, the Internet of Things (IoT), and smart automation. While these technologies offer improved efficiency and real-time control, they also introduce new vulnerabilities, particularly in systems that depend on centralized data and command structures. A malfunction or breach in the central system can lead to catastrophic outcomes, such as unplanned shutdowns, equipment damage, or even fatal accidents. In this context, decentralization offers a promising alternative by distributing control and decision-making across a network, thereby improving fault tolerance and system resilience.

Blockchain technology, originally developed for secure financial transactions, provides a decentralized, immutable ledger that records actions transparently and securely. When applied to industrial switch operations, blockchain can serve as a secure communication and control platform that ensures every action, whether it is switching on a motor, shutting down a system, or responding to sensor alerts, is authorized, logged, and verifiable. Smart contracts can further automate these actions based on pre-defined logic, reducing reliance on human intervention and minimizing delays in critical situations.

This paper proposes a system where remote switch operations are governed by blockchain-based smart contracts, with each command and response stored as a transaction on the ledger. The system integrates IoTenabled devices to monitor and control electrical switches, and uses edge computing to maintain low latency and ensure real-time responsiveness. By leveraging consensus mechanisms inherent in blockchain, unauthorized or suspicious commands can be detected and blocked before they affect the system.

One of the unique advantages of this approach is its ability to provide a transparent audit trail. Industrial supervisors and safety officers can trace every switch operation back to its origin, including the time, location, and identity of the operator or automated system that triggered it. This level of traceability is invaluable for ensuring compliance, facilitating post-incident analysis, and promoting continual safety improvement.

The remainder of the paper is structured as follows: Section II discusses related work and existing technologies in remote switch operation and industrial safety systems. Section III outlines the proposed system architecture, including the role of blockchain, IoT devices, and smart contracts. Section IV presents the implementation and testing methodology. Section V analyzes the results, highlighting improvements in safety, security, and performance. Finally, Section VI concludes the paper and suggests potential future enhancements, including the integration of machine learning and cross-platform blockchain interoperability.

By decentralizing remote switch operations, this research aims to redefine the future of industrial safety systems,

ensuring secure, efficient, and tamper-proof control across complex industrial environments.

## 2. Literature Review

The integration of blockchain technology with the Internet of Things (IoT) has emerged as a transformative solution to enhance data security, decentralization, and automation. Christidis and Devetsikiotis [1] highlighted how blockchain, combined with smart contracts, can facilitate autonomous transactions among IoT devices, eliminating the need for centralized control. This view is reinforced by Dorri et al. [2], who proposed a blockchain-based framework to improve the security and privacy of smart homes, addressing common vulnerabilities in centralized systems. The architectural considerations of such integrations have been systematically discussed by Xu et al. [3], offering a comprehensive model for blockchain application development. Kouicem et al. [4] provided a topdown review of IoT security issues, emphasizing the relevance of blockchain in addressing challenges related to data integrity and unauthorized access. Similarly, Zhang et al. [5] introduced a smart contract-based access control model for IoT, ensuring granular permissions and verifiable user actions.

Reyna et al. [6] explored both the opportunities and technical challenges of merging IoT with blockchain, while Yli-Huumo et al. [7] conducted a systematic review identifying gaps and future directions in blockchain research. Wang, Zhang, and Zhang [8] developed a blockchain-based fine-grained data-sharing framework, offering insights into decentralized access control. Casino, Dasaklis, and Patsakis [9] further categorized current blockchain applications, revealing key areas where integration with IoT has high potential. Moreover, Gai et al. [10] and Makhdoom et al. [11] emphasized the importance of edge computing and permissioned blockchains in enabling real-time and privacy-preserving smart grid operations. Collectively, these studies provide a solid foundation for understanding the convergence of blockchain and IoT in decentralized automation systems.

## 2. Methodology



Fig. 1: Project Block Diagram. ~46~

Figure 1 illustrates a decentralized, blockchain-based remote switch operation system designed to enhance industrial safety by allowing secure and remote activation of high-voltage electrical switches. The architecture leverages modern technologies, including IoT devices, blockchain nodes, galvanic isolation, smart contracts, and backend servers, to ensure operational integrity, security, and real-time monitoring.

#### 1. Remote Node (Frontend)

On the right side of the diagram, the Remote Node represents the user interface or control device, which can be a mobile phone, tablet, or industrial HMI (Human-Machine Interface) used by an operator. It enables personnel to control hazardous high-voltage switches without physically approaching the switchgear, ensuring safety in dangerous environments.

A message below the remote node states:

"In this system, there is no need to go in front of a switch; from any mobile/handheld device, we can operate any hazardous electrical switches."

This is crucial for preventing accidents and ensuring safety compliance in high-risk industrial areas, such as substations or control rooms with live components.

#### 2. Wi-Fi Router and Internet Access

The Wi-Fi router acts as the communication bridge between the remote node and the system controller. It enables the remote node to transmit instructions over the internet, which are then passed on to the backend, processed, and ultimately executed.

#### A labeled blue arrow says:

"Wi-Fi router: Provide internet to the system."

This ensures that the controller and the blockchain interface remain connected and in sync with real-time user commands and system logs.

#### 3. Encryption/Decryption Engine and Backend Server

In the central section of the diagram, the encryption/decryption engine is connected to a backend server. When a command is received from the remote node, the server first decrypts and validates the request.

A green note on the top left states:

"This is the backbone of the system. It receives the request, decrypts, and validates the packet. Once it is validated, it sends a request to the remote controller and saves the transaction to the blockchain."

This step is essential for ensuring security and integrity, preventing unauthorized access or malicious commands. It provides the system with a layered security model.

#### **4.** Blockchain Integration and Smart Contracts

At the heart of the system is the blockchain layer, represented by blocks labeled B0 to BN forming the Enterprise Blockchain. This ledger records each transaction, command, and operation. The process is managed through smart contracts, which are automated pieces of logic stored on the blockchain.

A text bubble states:

"It is responsible for saving transactions and providing history to the server when a request is received."

Smart contracts act as the decision-making layer that validates requests against preset conditions before allowing the switch to be operated. The blockchain ensures that every transaction is immutable, traceable, and verifiable. Another note emphasizes:

"This is a Blockchain node. Every transaction passes through encryption."

This guarantees that every action is audited and securely recorded, reinforcing transparency and compliance, especially in regulated industrial environments.

#### 5. Controller Subsystem

On the left side of the diagram, the Controller is a microcontroller or embedded processing unit responsible for executing the switching logic. It is connected to the Wi-Fi router and receives verified commands from the backend. The controller handles real-time signal processing.

#### It is annotated with:

"Process the remote request and trigger the load."

This means the controller acts on the validated request by sending signals to the driver module, which eventually actuates the switch.

#### 6. Galvanic Isolation

The system includes a Galvanic Isolation block between the controller and the driver. This is a critical safety feature that electrically isolates the control circuitry from the high-voltage actuation system, preventing reverse current flow or power surges from damaging sensitive electronics. A blue note states:

## "The system is fully Galvanic isolated, so that there are

no/very few chances to interfere with the sensitive system." This physical and electrical separation is particularly important in high-voltage industrial settings, as it safeguards both personnel and equipment.

## 7. Driver and High Voltage Switch

The Driver receives the PWM (Pulse Width Modulated) or digital signal from the controller (via galvanic isolation) and uses it to trigger the High Voltage Switch. This switch is capable of handling industrial loads such as transformers, circuit breakers, or large machinery.

An orange box says:

"It is responsible for driving the high voltage switch."

Just above this module, the switch is labeled with a highvoltage warning sign, indicating the dangerous nature of the component. Safety is maintained by ensuring remoteonly access through blockchain validation.

## 8. Blockchain Block Processing

The bottom section of the diagram shows the transaction processing and logging through the Enterprise Blockchain. Each block (B0 to BN) represents a step or a record of the transaction.

#### A note reads:

"Process the Remote request and trigger the load."

Each time a user sends a command; the event is logged into the next block in the chain. This structure maintains a chronological and tamper-proof record of all operations.

The blockchain ensures non-repudiation—meaning no operator can deny sending a command since every action is logged permanently.

#### 9. End-to-End Data Flow Summary

- 1. A remote user sends a command from a handheld device.
- 2. The command travels through the Wi-Fi router and reaches the backend server.
- 3. The Encryption/Decryption Engine decrypts and validates the request.
- 4. If valid, the backend logs the transaction to the blockchain and triggers the execution of a smart contract.
- 5. The smart contract forwards the instruction to the controller.

- 6. The controller, after checking safety conditions, sends a signal through the galvanic isolator to the driver.
- 7. The driver operates the high voltage switch.
- 8. The entire transaction is recorded on the Enterprise Blockchain for audit and traceability.

#### 4. Conclusion

This research presents a robust and secure decentralized architecture for remote switch operation in industrial environments, leveraging blockchain technology to address key challenges in safety, reliability, and traceability. Single points of failure, cyber vulnerabilities, and a lack of transparency often limit the effectiveness of traditional centralized systems. In contrast, the proposed blockchainbased approach ensures tamper-resistant data logging, decentralized control, and automated decision-making through the use of smart contracts. These features are crucial for enhancing safety in high-risk zones, where the manual operation of high-voltage switches poses a significant danger to human operators.

The integration of smart contracts enables automated, rulebased operations that significantly reduce the dependency on human intervention while maintaining operational accuracy and speed. The use of galvanic isolation ensures physical and electrical safety by protecting sensitive controller components from high-voltage surges. Edge computing support within the architecture ensures lowlatency responses, making the system suitable for real-time industrial applications. Additionally, the blockchain ledger provides a transparent and immutable audit trail for all transactions, thereby facilitating compliance, diagnostics, and accountability.

Testing in a simulated environment demonstrated that the system performs efficiently without compromising realtime responsiveness, making it a viable solution for various industrial automation scenarios. Future work may include incorporating AI and machine learning for predictive maintenance, enhancing system intelligence, and exploring interoperability across multiple blockchain networks. In essence, this work lays the groundwork for a new era of decentralized, secure, and intelligent industrial automation, focusing on safety and operational efficiency in Industry 4.0 and beyond.

#### References

- 1. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618–623.

https://doi.org/10.1109/PERCOMW.2017.7917634

- 3. Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer.
- Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of Things security: A top-down survey. Computer Networks, 141, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012
- 5. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the

Internet of Things. IEEE Internet of Things Journal, 6(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705

- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PLoS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477
- Wang, S., Zhang, Y., & Zhang, Y. (2019). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 6, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
- Gai, K., Wu, Y., Zhu, L., Xu, L., & Zhang, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet of Things Journal, 6(5), 7992–8004. https://doi.org/10.1109/JIOT.2019.2911053
- Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019
- Samaniego, M., & Deters, R. (2016). Blockchain as a service for IoT. 2016 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom), 433– 436. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.101
- Al-Bassam, M. (2018). SCPKI: A smart contract-based PKI and identity system. Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 35–40. https://doi.org/10.1145/3211933.3211939
- Liang, X., Zhao, J., Shetty, S., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 1–5. https://doi.org/10.1109/PIMRC.2017.8292361

International Congress on Big Data (BigData Congress), 557–564.
 International Congress on Big Data (BigData Congress), 557–564.

- https://doi.org/10.1109/BigDataCongress.2017.85
  16. Singh, S., Jeong, Y. S., & Park, J. H. (2020). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200–222. https://doi.org/10.1016/j.jnca.2016.09.002
- 17. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Blockchain for 5G and beyond

networks: A state of the art survey. Journal of Network and Computer Applications, 166, 102693. https://doi.org/10.1016/j.jnca.2020.102693

- Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, Finance and Management, 25(1), 18–27. https://doi.org/10.1002/isaf.1424
- Alharby, M., & Van Moorsel, A. (2017). Blockchainbased smart contracts: A systematic mapping study. arXiv preprint arXiv:1710.06372. https://arxiv.org/abs/1710.06372
- Wang, H., & Liu, X. (2021). Blockchain and industrial IoT for automation and manufacturing. Journal of Industrial Information Integration, 22, 100200. https://doi.org/10.1016/j.jii.2020.100200
- Chakraborty, S., & Aithal, P. S. (2023). Let Us Create an Alexa-Enabled IoT Device Using C#, AWS Lambda and ESP Module. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(3), 256-261. DOI: https://doi.org/10.5281/zenodo.8260291
- 22. Chakraborty, S., & Aithal, P. S. (2023). Alexa Enabled IoT Device Simulation Using C# And AWS Lambda. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(3), 359-368. DOI: https://doi.org/10.5281/zenodo.8329375
- Chakraborty, S. & Aithal, P. S. (2023). Smart Magnetic Door Lock for Elderly People Using AWS Alexa, IoT, Lambda and ESP Module. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(4), 474-483. DOI: https://doi.org/10.5281/zenodo.10467946
- 24. Chakraborty, S., & Aithal, P. S. (2023). IoT-Based Switch Board for Kids Using ESP Module And AWS. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(3), 248-254. DOI: https://doi.org/10.5281/zenodo.8285219
- 25. Chakraborty, S. & Aithal, P. S. (2024). AI Kitchen. International Journal of Applied Engineering and Management Letters (IJAEML), 8(1), 128-137. DOI: https://doi.org/10.5281/zenodo.10810228
- Chakraborty, S., & Aithal, P. S. (2023). IoT-Based Industrial Debug Message Display Using AWS, ESP8266 And C#. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(3), 249-255. DOI: https://doi.org/10.5281/zenodo.8250418
- Chakraborty, S., & Aithal, P. S., (2023). Let Us Create Our Desktop IoT Soft-Switchboard Using AWS, ESP32 and C#. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(3), 185-193. DOI: https://doi.org/10.5281/zenodo.8234036
- Chakraborty, Sudip, & Aithal, P. S., (2021). An Inverse Kinematics Demonstration of a Custom Robot using C# and CoppeliaSim. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 5(1), 78-87. DOI: http://doi.org/10.5281/zenodo.4755778.
- 29. Chakraborty, S., & Aithal, P. S., (2023). MVVM Demonstration Using C# WPF. International Journal of Applied Engineering and Management Letters (IJAEML), 7(1), 1-14. DOI: https://doi.org/10.5281/zenodo.7538711

- Chakraborty, S., & Aithal, P. S. (2023). Let Us Create A Lambda Function for Our IoT Device In The AWS Cloud Using C#. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(2), 145-155. DOI: https://doi.org/10.5281/zenodo.7995727
- Chakraborty, S., & Aithal, P. S., (2022). How to make IoT in C# using Sinric Pro. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 6(2), 523-530. DOI: https://doi.org/10.5281/zenodo.7335167
- Chakraborty, S., & Aithal, P. S., (2022). Virtual IoT Device in C# WPF Using Sinric Pro. International Journal of Applied Engineering and Management Letters (IJAEML), 6(2), 307-313. DOI: https://doi.org/10.5281/zenodo.7473766
- 33. Chakraborty, S. & Aithal, P. S. (2023). Let Us Create an Alexa Skill for Our IoT Device Inside the AWS Cloud. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(2), 214-225. DOI: https://doi.org/10.5281/zenodo.7940237
- Chakraborty, Sudip, & Aithal, P. S., (2021). Forward Kinematics Demonstration of 6DF Robot using CoppeliaSim and C#. International Journal of Applied Engineering and Management Letters (IJAEML), 5(1), 29-37. DOI: http://doi.org/10.5281/zenodo.4680570.
- 35. Chakraborty, S., & Aithal, P. S., (2023). Let Us Create a Physical IoT Device Using AWS and ESP Module. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(1), 224-233. DOI: https://doi.org/10.5281/zenodo.7779097
- Chakraborty, S., & Aithal, P. S., (2023). Let Us Create An IoT Inside the AWS Cloud. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(1), 211-219. DOI: https://doi.org/10.5281/zenodo.7726980
- 37. Chakraborty, S., & Aithal, P. S., (2023). Let Us Create Multiple IoT Device Controller Using AWS, ESP32 And C#. International Journal of Applied Engineering and Management Letters (IJAEML), 7(2), 27-34. DOI: https://doi.org/10.5281/zenodo.7857660
- Chakraborty, Sudip, & Aithal, P. S., (2021). A Custom Robotic ARM in CoppeliaSim. International Journal of Applied Engineering and Management Letters (IJAEML), 5(1), 38-50. DOI: http://doi.org/10.5281/zenodo.4700297.
- Chakraborty, Sudip, & Aithal, P. S., (2021). Forward and Inverse Kinematics Demonstration using RoboDK and C#. International Journal of Applied Engineering and Management Letters (IJAEML), 5(1), 97-105. DOI: http://doi.org/10.5281/zenodo.4939986.
- 40. Chakraborty, S., & Aithal, P. S., (2022). A Practical Approach To GIT Using Bitbucket, GitHub and SourceTree. International Journal of Applied Engineering and Management Letters (IJAEML), 6(2), 254-263. DOI: https://doi.org/10.5281/zenodo.7262771

41. Chakraborty, S. & Aithal, P. S. (2024). WhatsApp

- Based Notification on Low Battery Water Level Using ESP Module and TextMeBOT. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 8(1), 291-309. DOI: https://doi.org/10.5281/zenodo.10835097
- 42. Chakraborty, S. & Aithal, P. S. (2024). Go Green: ReUse LED Tube Light and Make it WhatsApp

Enabled Using ESP Module, Twilio, and ThingESP. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 8(2), 296-310. DOI: https://doi.org/10.5281/zenodo.11204974

- 43. Chakraborty, S. & Aithal, P. S. (2024). Let Us Build a MQTT Pub-Sub Client In C# For IoT Research. International Journal of Management, Technology, and Social Sciences (IJMTS), 9(1), 104-114. DOI: https://doi.org/10.5281/zenodo.10603409
- Chakraborty, S. & Aithal, P. S. (2024). Autonomous Fever Monitoring System For Child Using Arduino, ESP8266, WordPress, C# And Alexa. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 8(1), 135-144. DOI: https://doi.org/10.5281/zenodo.10710079
- 45. Chakraborty, S. & Aithal, P. S. (2024). Smart LPG Leakage Monitoring and Control System Using Gas Sensor (MQ-X), AWS IoT, and ESP Module. International Journal of Applied Engineering and Management Letters (IJAEML), 8(1), 101-109. DOI: https://doi.org/10.5281/zenodo.10718875
- 46. Chakraborty, S., & Aithal, P. S. (2024). Communication Channels Review For ESP Module Using Arduino IDE And NodeMCU. International Journal of Applied Engineering and Management Letters (IJAEML), 8(1), 1-14. DOI: https://doi.org/10.5281/zenodo.10562843
- 47. Chakraborty, S., & Aithal, P. S. (2023). CRUD Operation on WordPress Database Using C# SQL Client. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(4), 138-149. DOI: https://doi.org/10.5281/zenodo.10162719
- 48. Chakraborty, S., & Aithal, P. S., (2023). CRUD Operation On WordPress Database Using C# And REST API. International Journal of Applied Engineering and Management Letters (IJAEML), 7(4), 130-138. DOI: https://doi.org/10.5281/zenodo.10197134
- 49. Chakraborty, S., & Aithal, P. S., (2023). CRUD Operation on WordPress Posts From C# over REST API. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(4), 223-231. DOI: https://doi.org/10.5281/zenodo.10264407
- Chakraborty, S. & Aithal, P. S. (2023). CRUD Operation On WordPress Custom Post Type (CPT) From C# Over REST API. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(4), 323-331. DOI: https://doi.org/10.5281/zenodo.10408545
- 51. Chakraborty, S. & Aithal, P. S. (2023). Let Us Build a WordPress Custom Post Type (CPT). International Journal of Applied Engineering and Management Letters (IJAEML), 7(4), 259-266. DOI: https://doi.org/10.5281/zenodo.10440842
- 52. Chakraborty, S. & Aithal, P. S. (2024). Let Us Manage BP Monitor Data Using WordPress Server and C#. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 8(1), 1-9. DOI: https://doi.org/10.5281/zenodo.10551926
- Chakraborty, S. & Aithal, P. S. (2024). Don't Worry; AI will Take Care of Your Sweet Home. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 8(1), 240-250. DOI: https://doi.org/10.5281/zenodo.10780905

- Chakraborty, S. & Aithal, P. S. (2024). AI Bedroom. International Journal of Applied Engineering and Management Letters (IJAEML), 8(1), 110-119. DOI: https://doi.org/10.5281/zenodo.10780920
- 55. Chakraborty, S., & Aithal, P. S. (2023). How To Create Our Custom Model in CoppeliaSim From 3D File. International Journal of Applied Engineering and Management Letters (IJAEML), 7(2), 164-174. DOI: https://doi.org/10.5281/zenodo.8117666
- 56. Chakraborty, S., & Aithal, P. S. (2023). Smart Home Simulation in CoppeliaSim Using C# Through WebSocket. International Journal of Applied Engineering and Management Letters (IJAEML), 7(2), 134-143. DOI: https://doi.org/10.5281/zenodo.8075717
- Chakraborty, S., & Aithal, P. S. (2023). Automated Test Equipment Simulation In CoppeliaSim Using C# Over WebSocket. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(2), 284-291. DOI: https://doi.org/10.5281/zenodo.8117650
- Chakraborty, S., & Aithal, P. S. (2023). Industrial Automation Debug Message Display Over Modbus RTU Using C#. International Journal of Management, Technology, and Social Sciences (IJMTS), 8(2), 305-313. DOI: https://doi.org/10.5281/zenodo.8139709
- 59. Chakraborty, S., & Aithal, P. S. (2023). Modbus Data Provider for Automation Researcher Using C#. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(3), 1-7. DOI: https://doi.org/10.5281/zenodo.8162680
- Sudip Chakraborty, & Aithal, P. S., (2021). Demonstration of Modbus Protocol for Robot Communication Using C#. International Journal of Applied Engineering and Management Letters (IJAEML), 5(2), 119-131. DOI: https://doi.org/10.5281/zenodo.5709235