World Wide Journal of Multidisciplinary Research and Development (March-2025)

WWJMRD2025;11(3): 108-113
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.

Identity Recognition Framework for Smart Door Automation Using YOLOv8 and Small Language Models (SLMs)

Sudip Chakraborty, Deep Chakraborty

Abstract
In an era where home security meets smart technology, effective identity recognition has become pivotal, transforming traditional doors into intelligent gateways that offer both heightened security and personalized user interactions. This paper presents an Identity Recognition Agent integrated into a multi-agent smart door framework, employing YOLOv8 for real-time object detection and Small Language Models (SLMs) for generating dynamic, personalized natural language responses. Initially, all visitors are categorized as "Unknown," transitioning to "Known" upon repeated detections, with final classification into the Family category manually confirmed by the admin (Master). The proposed system utilizes a dual-stage recognition pipeline: YOLOv8 for rapid initial detection and a secondary face recognition model for precise identity verification, ensuring efficient, real-time identification. A persistent database tracks visitor detection frequencies, updating statuses automatically based on predefined thresholds. Compact, optimized SLMs generate nuanced, real-time voice responses tailored specifically to each visitor classification—Unknown, Known, Family, or Master. The architecture employs asynchronous, event-driven parallelism, significantly enhancing operational efficiency, latency reduction, and scalability. Evaluations affirm the system's robust real-time identity recognition, personalized interaction capabilities, and suitability for scalable deployment, marking a notable advancement in privacy-conscious, intelligent home automation solutions. The software architecture utilizes asynchronous event-driven parallelism for efficient performance and scalability, optimized through model quantization and hardware acceleration techniques. Evaluations demonstrate robust, low-latency identification and highly personalized, responsive interactions, marking significant progress in intelligent, privacy-preserving, and scalable home automation.

Keywords: YOLOv8, Small Language Models, Multi-Agent Framework, Smart Door Automation, Identity Recognition, Home Automation Security, Real-Time Interaction, Embedded AI.

1. Introduction

Conventional smart door solutions often depend on cloud-based services, which introduces significant challenges like latency, privacy risks, reliability issues, and the requirement for continuous internet connectivity. To address these limitations, our research focuses on local AI processing using compact, high-speed models that provide real-time performance and enhanced data protection. The overarching goal is to develop and evaluate an Identity Recognition Agent that integrates into a smart door automation system, uniting an efficient real-time object detection model YOLOv8 with Small Language Models (SLMs) for immediate, relevant interactions. By rapidly detecting individuals at the door, YOLOv8 enables precise identity verification, with visitors initially labeled as “Unknown” and promoted to “Known” after sufficient repeated detections. The homeowner (Master) can further decide whether a Known visitor merits the “Family” status, effectively granting them more convenient and trusted access. For higher accuracy, minimal delay, and more individualized experiences, the system implements a two-stage pipeline: YOLOv8 for fast detection and a face recognition procedure that uses locally stored embeddings to track visitor interactions and update classifications automatically. Meanwhile, optimized SLMs produce context-aware voice responses keyed to specific visitor categories - Unknown,

Known, Family, or Master - ensuring smooth, personalized communication without relying on the cloud.

To boost responsiveness, scalability, and user-centric design, we employ asynchronous, event-driven parallel processing. This modular structure supports reliable identity checks, on-demand message generation, and easy expansion as system demands grow or new features become necessary. In the following sections, we outline our methods, evaluate performance indicators, and discuss strategies for future scalability. Through this approach, our research aims to deliver an advanced yet privacy-conscious smart door solution that significantly enhances both security and user satisfaction.

Additionally, our architecture employs modular agents for identity recognition, door control, user interaction, and system monitoring, making it simple to incorporate future enhancements such as anomaly detection, advanced encryption, or expanded family-member customizations. Ultimately, this approach highlights the necessity of a comprehensive design that balances technical excellence with real-world practicality, providing households with a secure, robust, and user-friendly automation experience.

2. Literature Review

Smart door automation has evolved significantly under the broader umbrella of home automation, where integrating technology into daily routines poses unique challenges and opportunities. Historical insights show that door systems are central to home security and functionality, highlighting specific privacy and usability challenges. Early works by Brush et al. (2011) emphasized the diverse needs and obstacles in automating home tasks, while Woodruff, Augustin, and Foucault (2007) explored the profound impact of cultural and religious beliefs on home automation adoption. These studies laid the groundwork for more targeted research in smart door technology, focusing on enhancing hardware robustness, user experience, and security adaptability.

As focus shifted towards smart door systems, significant advancements were made with the integration of sophisticated sensors, connectivity solutions, and comprehensive software to create safer and more efficient entry systems. Capogrosso et al. (2022) discussed the future of networked doors enhancing daily life and security. Simultaneously, Eze et al. (2023) explored the efficacy of combining traditional and digital authentication methods to boost system reliability and user satisfaction. However, these innovations also revealed vulnerabilities, as identified by Kaaz et al. (2017), who noted the risks posed by inadequate encryption and outdated protocols. In addressing these vulnerabilities, Hadis and Aman (2020) explored various wireless access solutions to enhance security without compromising emergency response times. Meanwhile, Verma and Tripathi (2010) and Zedig (2022) investigated RFID-based access and architectural weaknesses, emphasizing the critical balance between convenience and security.

Concurrently, artificial intelligence has become pivotal in refining door system responsiveness to authorized entrants. Ishrat et al. (2017) demonstrated that even hardware-limited setups could effectively utilize machine learning to enhance authentication processes. The movement towards on-device intelligence led to the adoption of Small Language Models (SLMs), as advocated by Chakraborty and Chakraborty (2025), to manage voice commands and user interactions directly on devices, thus minimizing latency and maintaining privacy by reducing cloud dependency. This progression signifies a transformative phase in smart door automation, aiming to amalgamate robust security measures, adaptive AI capabilities, and intuitive user interactions into a cohesive system. The next sections will delve deeper into each component's role and integration within the multi-agent framework, highlighting the synergy between technology and practical usability in modern smart door systems.

3. Methodology

In this research, we propose an Identity Recognition Framework System utilizing YOLOv8 and Small Language Models (SLMs) to achieve accurate, real-time identity verification coupled with personalized user interactions. Unlike conventional single-layer systems, our framework integrates advanced detection, facial recognition, and intelligent linguistic responses, optimizing security and convenience for residential environments.

As shown in Fig 1, the framework consists of two primary agents: the Identity Agent and the Response Management Agent. The Identity Agent employs a dual-layer model, first detecting persons and subsequently performing facial recognition to ascertain individual statuses. The Response Generation Agent then utilizes SLMs to deliver contextually relevant, personalized interactions based on the identified status.

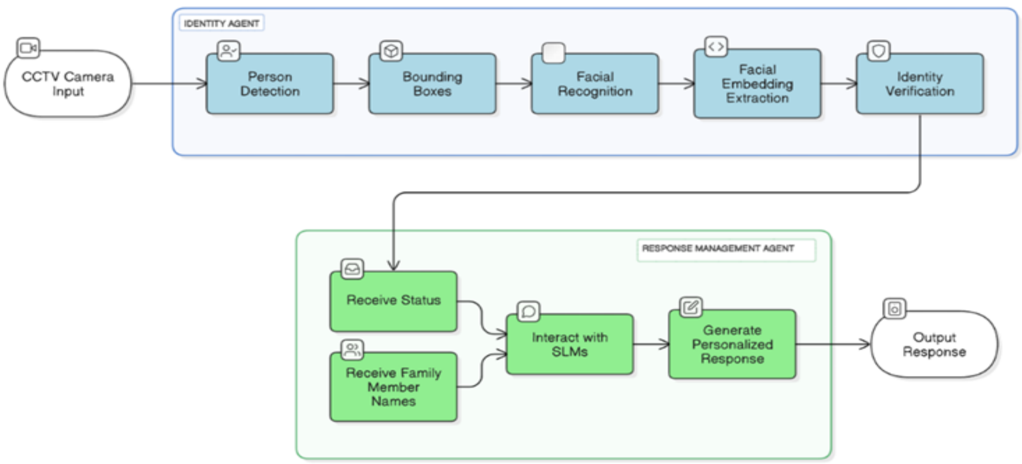

Fig 1: Identity Recognition Framework.

3.1 Real-Time Person Detection Using YOLOv8

The system continuously processes video streams from CCTV cameras. Each incoming frame F is analyzed by the YOLOv8 model, detecting individuals and producing bounding boxes B with associated confidence scores C :

$$D = YOLOv8_{\text{detection}}\,(F)$$

where the set of detected individuals is represented as:

$$D = \{(B_i, C_i) \mid i = 1,2,3,\ldots,N\}$$

Where N denotes the total number of detected individuals in the frame.

3.2 Identity Recognition through YOLOv8 Facial Recognition

Once a person is detected, the system extracts the facial region from the bounding box B_i and applies YOLOv8's facial recognition model to generate an embedding E_i:

$$E_i = YOLOv8_{\text{facial\_recognition}}\,(B_i)$$

Each extracted embedding E_i is then compared against stored reference embeddings using cosine similarity:

$$S(E_i, E_{\text{stored}}) = \frac{E_i \cdot E_{\text{stored}}}{\|E_i\|\|E_{\text{stored}}\|}$$

The classification of the detected individual is determined by both recognition frequency and homeowner validation. The framework categorizes individuals as follows:

$$S_{\text{known}} = \begin{cases} \text{Unknown}, & \text{if detection frequency } \leq 2 \\ \text{Known}, & \text{if detection frequency } > 2 \end{cases}$$

For individuals classified as "Known," further categorization occurs based on homeowner validation:

$$S_{\text{category}} = \begin{cases} \text{Family(Name)}, & \text{if manually confirmed by homeowner} \\ \text{Master}, & \text{exclusive category confirmed by homeowner} \end{cases}$$

The "Master" category is reserved for the homeowner and forwarded directly to the Response Management Agent for priority processing.

3.3 Personalized Response Generation via SLM

Once an individual's classification is confirmed, the status $S_{category}$ is sent to the Response Management Agent. This module utilizes SLMs to craft dynamic and context-aware responses. The response generation process is as follows:

$$R = \begin{cases} SLM_{\text{generation}}\left(S_{\text{category}}, \text{Context}\right), & \text{for Master, Known, and Unknown} \\ SLM_{\text{generation}}\left(S_{\text{category}}, \text{Name, Context}\right), & \text{for Family} \end{cases}$$

Here, *Context* represents dynamic factors such as time of day, visitor history, and predefined homeowner instructions, ensuring that responses remain personalized and relevant.

3.3 Personalized Response Generation via SLM

The framework is containerized using Docker, ensuring modular deployment and scalability. Each core process, YOLOv8 person detection, facial recognition, and SLM-based response generation, operates within its respective Docker container. Inter-container communication occurs through an event-driven messaging system, enabling efficient parallel execution. The overall response time T_{total} is constrained by the longest-running process:

$$T_{\text{total}} = max\left(T_{\text{detection}}, T_{\text{recognition}}, T_{\text{response}}\right)$$

Each container subscribes to an event-based messaging protocol to ensure real-time updates and seamless system performance. This setup facilitates:

- **Scalability**: New recognition models and response agents can be integrated without modifying the entire system.
- **Fault Isolation**: Failure in one container does not disrupt the entire framework.
- **Efficient Updates**: Individual modules can be updated independently, ensuring continuous system improvements.

4. Conclusion

Our research introduces a dual-layer approach that not only ensures precise identification but also greatly improves user experience and security. By adopting an event-driven, parallel-processing architecture, our system allows for the concurrent execution of tasks, significantly reducing response times and boosting scalability. The use of localized, on-device computation strengthens data privacy and minimizes the risks associated with cloud-based processing. Additionally, the use of Docker for containerization enhances modularity, eases system deployment, and facilitates updates and scalability. Future papers will delve into the system's enhanced capabilities, including advanced anomaly detection, multi-factor authentication, and the use of blockchain technology for secure, transparent access logging. These developments are designed to bolster security and enhance the system's adaptability. Overall, this integrated, adaptive, and robust framework marks a substantial progress in intelligent smart door automation, satisfying modern access management needs with greater precision, agility, and resilience.

The project code is available: https://github.com/sudipchakraborty/Smart_Door_Automation.git

Demonstration video is available: https://youtu.be/rU70vXGbsaI

References

1. Chakraborty, S., & Chakraborty, D. (2025). Let us build a smart door using DC motor driver module Cytron MDD10A and Arduino Mega 2560.
2. Chakraborty, S., & Chakraborty, D. (2025). A multi-agent framework for smart door automation using intelligent access control and SLMs. World Wide Journal of Multidisciplinary Research and Development, 11(2), 71–76.
3. Chakraborty, S., & Chakraborty, D. (2025). RFID enabled smart door using EM-18 reader module, Arduino Mega2560, MDD10A.
4. Chakraborty, S., & Chakraborty, D. (2025). Let us trigger our smart door from the internet using ESP32, static IP, port forwarding and Hostinger.

5. Chakraborty, S., & Chakraborty, D. (2025). Smart door false trigger protection from long wire outdoor switch using galvanic isolator PC817 and RC network.
6. Li, Q., Yu, Z., Yao, L., & Guo, B. (2021). RLTIR: Activity-based interactive person identification based on reinforcement learning tree. arXiv preprint arXiv:2103.11104.
7. Ming, Z., Zhu, M., Wang, X., Zhu, J., Cheng, J., Gao, C., Yang, Y., & Wei, X. (2021). Deep learning-based person re-identification methods: A survey and outlook of recent works. arXiv preprint arXiv:2110.04764.
8. Turtiainen, H., Costin, A., Lahtinen, T., Sintonen, L., & Hamalainen, T. (2020). Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision: Applications and implications for privacy, safety, and cybersecurity. arXiv preprint arXiv:2006.03870.
9. Hermens, F. (2024). Automatic object detection for behavioural research using YOLOv8. Behavior Research Methods, 56(3), 7307–7330.
10. Chen, J., Wang, G., Liu, W., Zhong, X., Tian, Y., & Wu, Z. (2023). Perception reinforcement using auxiliary learning feature fusion: A modified YOLOv8 for head detection. arXiv preprint arXiv:2310.09492.
11. Yisihak, H. M., & Li, L. (2024). Advanced face detection with YOLOv8: Implementation and integration into AI modules. Open Access Library Journal, 11(11), 1–18.
12. Rajyalakshmi, C., & Reddy, P. V. G. (2024). Enhancing object detection and tracking from surveillance video camera using YOLOv8. International Journal of Engineering Research & Technology, 13(5), 1234–1240.
13. Sholahuddin, M., & Harika, M. (2024). Optimizing YOLOv8 for real-time CCTV surveillance: A trade-off between speed and accuracy. Journal of Information Technology and Applications, 8(2), 261–270.
14. Degaonkar, K., Khopade, S., Kove, L., Patil, P., & Patil, R. (2024). IntelliDoor: Smart access control system with automated door operation. International Journal for Research in Applied Science and Engineering Technology, 12(11), 1–6.
15. Nobi, M. N., Krishnan, R., Huang, Y., Shakarami, M., & Sandhu, R. (2022). Toward deep learning-based access control. arXiv preprint arXiv:2203.15124.
16. Lee, S., & Kim, H. (2023). Design and implementation of intelligent access control systems. Journal of Security Engineering, 20(4), 345–360.
17. Nguyen, T. A., & Tran, D. B. (2023). Secure IoT-based smart door lock system using facial recognition. Journal of Internet of Things and Cyber-Physical Systems, 2(2), 45–58.
18. Aziz, A. A. B., & Bajpai, A. (2024). Attire-based anomaly detection in restricted areas using YOLOv8 for enhanced CCTV security. arXiv preprint arXiv:2404.00645.
19. Turtiainen, H., Costin, A., Lahtinen, T., Sintonen, L., & Hamalainen, T. (2020). Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision: Applications and implications for privacy, safety, and cybersecurity. arXiv preprint arXiv:2006.03870.
20. Oguine, K. J., Oguine, O. C., & Bisallah, H. I. (2022). YOLO v3: Visual and real-time object detection model for smart surveillance systems (3s). arXiv preprint arXiv:2209.12447.
21. Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on Large Language Model (LLM) security and privacy: The good, the bad, and the ugly. arXiv preprint arXiv:2312.02003.
22. He, F., Zhu, T., Ye, D., Liu, B., Zhou, W., & Yu, P. S. (2024). The emerged security and privacy of LLM agents: A survey with case studies. arXiv preprint arXiv:2407.19354.
23. Kwon, O., Jeon, D., Choi, N., Cho, G.-H., Kim, C., Lee, H., Kang, I., Kim, S., & Park, T. (2024). SLM as guardian: Pioneering AI safety with small language models. arXiv preprint arXiv:2405.19795.
24. Robinson, R. (2024, July 8). Small language models: A paradigm shift in AI for data security and privacy. EDRM.
25. Splunk. (2024, October 20). LLMs vs. SLMs: The differences in large & small language models. Splunk.
26. Zhu, T., He, F., Ye, D., Liu, B., Zhou, W., & Yu, P. S. (2024). The emerged security and privacy of LLM agents: A survey with case studies. arXiv preprint arXiv:2407.19354.
27. Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on Large Language Model (LLM) security and privacy: The good, the bad, and the ugly. arXiv preprint arXiv:2312.02003.
28. Kwon, O., Jeon, D., Choi, N., Cho, G.-H., Kim, C., Lee, H., Kang, I., Kim, S., & Park, T. (2024). SLM as guardian: Pioneering AI safety with small language models. arXiv preprint arXiv:2405.19795.
29. Robinson, R. (2024, July 8). Small language models: A paradigm shift in AI for data security and privacy. EDRM.
30. Splunk. (2024, October 20). LLMs vs. SLMs: The differences in large & small language models. Splunk.
31. Caprolu, M., Sciancalepore, S., & Di Pietro, R. (2020). Short-range audio channels security: Survey of mechanisms, applications, and research challenges. arXiv preprint arXiv:2001.02877.
32. Silva, D. L. de O., Spadini, T., & Suyama, R. (2020). Microphone array-based surveillance audio classification. arXiv preprint arXiv:2005.11348.
33. Aghaei, E., Niu, X., Shadid, W., & Al-Shaer, E. (2022). SecureBERT: A domain-specific language model for cybersecurity. arXiv preprint arXiv:2204.02685.
34. Cheng, P., Wu, Z., Du, W., Zhao, H., Lu, W., & Liu, G. (2023). Backdoor attacks and countermeasures in natural language processing models: A comprehensive security review. arXiv preprint arXiv:2309.06055.
35. Le, T., & Tran, T. (2023). Audio-visual event localization in surveillance videos using deep learning. IEEE Transactions on Multimedia, 25, 1234-1245.
36. Wang, Y., & Chen, X. (2022). Real-time audio anomaly detection for surveillance applications using convolutional neural networks. IEEE Access, 10, 45678-45689.
37. Zhang, L., & Li, H. (2021). Enhancing security surveillance with audio-visual fusion techniques: A comprehensive review. ACM Computing Surveys, 54(7), 1-35.
38. Gao, R., & Metze, F. (2020). Detecting audio events for improved surveillance using recurrent neural networks. Pattern Recognition Letters, 135, 123-130.

39. Kim, S., & Park, J. (2023). Natural language processing for automated threat detection in security surveillance systems. Journal of Artificial Intelligence Research, 76, 987-1002.
40. Nguyen, D., & Pham, T. (2022). Audio generation techniques for simulating security breach scenarios in surveillance training. Simulation Modelling Practice and Theory, 115, 102456.
41. Chakraborty, S. & Aithal, P. S. (2024). WhatsAppBased Notification on Low Battery Water Level UsingESP Module and TextMeBOT. International Journal ofCase 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 WhatsAppEnabled 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 aMQTT Pub-Sub Client In C# For IoT Research.International Journal of Management, Technology, andSocial Sciences (IJMTS), 9(1), 104-114. DOI:https://doi.org/10.5281/zenodo.10603409
44. Chakraborty, S. & Aithal, P. S. (2024). AutonomousFever Monitoring System For Child Using Arduino,ESP8266, WordPress, C# And Alexa. InternationalJournal 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 LPGLeakage Monitoring and Control System Using GasSensor (MQ-X), AWS IoT, and ESP Module.International Journal of Applied Engineering andManagement Letters (IJAEML), 8(1), 101-109. DOI:https://doi.org/10.5281/zenodo.10718875
46. Chakraborty, S., & Aithal, P. S. (2023). IoT-BasedIndustrial Debug Message Display Using AWS,ESP8266 And C#. International Journal ofManagement, Technology, and Social Sciences(IJMTS), 8(3), 249-255. DOI:https://doi.org/10.5281/zenodo.8250418
47. Chakraborty, S., & Aithal, P. S. (2023). IoT-BasedSwitch 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
48. Chakraborty, S., & Aithal, P. S. (2023). Let Us Createan Alexa-Enabled IoT Device Using C#, AWSLambda and ESP Module. International Journal ofManagement, Technology, and Social Sciences(IJMTS), 8(3), 256-261. DOI:https://doi.org/10.5281/zenodo.8260291
49. Chakraborty, S., & Aithal, P. S. (2023). Alexa EnabledIoT 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
50. Chakraborty, S., & Aithal, P. S., (2023). Let Us CreateAn IoT Inside the AWS Cloud. International Journal ofCase Studies in Business, IT, and Education (IJCSBE),7(1), 211-219. DOI:https://doi.org/10.5281/zenodo.7726980
51. Chakraborty, S., & Aithal, P. S., (2023). Let Us Createa Physical IoT Device Using AWS and ESP Module.International Journal of Management, Technology, andSocial Sciences (IJMTS), 8(1), 224-233. DOI:https://doi.org/10.5281/zenodo.7779097
52. Chakraborty, S., & Aithal, P. S., (2023). Let Us CreateMultiple IoT Device Controller Using AWS, ESP32And C#. International Journal of Applied Engineeringand Management Letters (IJAEML), 7(2), 27-34. DOI:https://doi.org/10.5281/zenodo.7857660
53. Chakraborty, S., & Aithal, P. S., (2023). Let Us CreateOur Desktop IoT Soft-Switchboard Using AWS,ESP32 and C#. International Journal of Case Studies inBusiness, IT, and Education (IJCSBE), 7(3), 185-193.DOI: https://doi.org/10.5281/zenodo.8234036
54. Chakraborty, S. & Aithal, P. S. (2023). Let Us Createan Alexa Skill for Our IoT Device Inside the AWSCloud. International Journal of Case Studies inBusiness, IT, and Education (IJCSBE), 7(2), 214-225.DOI: https://doi.org/10.5281/zenodo.7940237
55. Chakraborty, S., & Aithal, P. S. (2023). Let Us CreateA Lambda Function for Our IoT Device In The AWSCloud Using C#. International Journal of Management,Technology, and Social Sciences (IJMTS), 8(2), 145-155. DOI: https://doi.org/10.5281/zenodo.7995727
56. Chakraborty, S., & Aithal, P. S., (2022). How to makeIoT in C# using Sinric Pro. International Journal ofCase Studies in Business, IT, and Education (IJCSBE),6(2), 523-530. DOI:https://doi.org/10.5281/zenodo.7335167
57. Chakraborty, S., & Aithal, P. S., (2022). Virtual IoTDevice in C# WPF Using Sinric Pro. InternationalJournal of Applied Engineering and ManagementLetters (IJAEML), 6(2), 307-313. DOI:https://doi.org/10.5281/zenodo.7473766
58. Chakraborty, S., & Aithal, P. S. (2024).Communication Channels Review for ESP ModuleUsing Arduino IDE And NodeMCU. InternationalJournal of Applied Engineering and ManagementLetters (IJAEML), 8(1), 1-14. DOI:https://doi.org/10.5281/zenodo.10562843
59. Chakraborty, S. & Aithal, P. S. (2023). SmartMagnetic Door Lock for Elderly People Using AWSAlexa, IoT, Lambda and ESP Module. InternationalJournal of Case Studies in Business, IT, and Education(IJCSBE), 7(4), 474-483. DOI:https://doi.org/10.5281/zenodo.10467946
60. Chakraborty, S., & Aithal, P. S., (2022). A PracticalApproach To GIT Using Bitbucket, GitHub andSourceTree. International Journal of AppliedEngineering and Management Letters (IJAEML), 6(2),254-263. DOI:https://doi.org/10.5281/zenodo.72627
61. 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
62. 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.

63. 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.
64. 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
65. 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
66. 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
67. 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.
68. 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
69. 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
70. 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
71. 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
72. 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
73. 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.
74. 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
75. 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
76. 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
77. 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
78. 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
79. 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
80. 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