WWJMRD 2025; 11(02): 71-76
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.

A Multi-Agent Framework for Smart Door Automation Using Intelligent Access Control and SLMs

Sudip Chakraborty, Deep Chakraborty

Abstract
Recent advancements in home automation have highlighted the growing importance of secure and intelligent door management systems, where maintaining user convenience and data privacy is paramount. Building on prior research into smart door controls and automated security solutions, this paper introduces a novel multi-agent framework that leverages Small Language Models (SLMs) for real-time decision-making and user interaction. Unlike larger, more resource-intensive language models, SLMs offer lower latency and reduced computational overhead, making them better suited for on-device operation. To distribute tasks and optimize performance, the system comprises five specialized agents—Central Door Management, Response Management, Door Control, Identity Recognition, and Audio Response. The Identity Recognition Agent leverages advanced vision-based techniques (such as YOLO) to classify visitors (e.g., family, friends, or unknown), while the Response Management and Audio Response Agents employ SLMs to deliver contextually relevant, voice-based instructions. By offloading targeted language processing tasks to smaller, domain-focused models, the system effectively mitigates network dependencies, improving security and privacy. Preliminary evaluations indicate that this architecture not only maintains robust access control and personalized interaction but also exhibits strong scalability for diverse household scenarios. Overall, our findings suggest that a multi-agent design, powered by SLMs, represents a promising direction for next-generation smart door automation and security solutions.

Keywords: Smart Door, Multi-Agent Framework, SLM for Home Automation, AI in Security, Voice Interface, Home Automation, Intelligent Access Control.

1. Introduction

Smart door automation has emerged as a key component of modern smart homes, enhancing security, convenience, and user experience. Research in this domain has explored various techniques for automating door locks, improving authentication methods, and integrating these systems with broader home automation frameworks. Early studies, for instance, identified both the potential and challenges of adopting home automation "in the wild," noting issues around usability, privacy, and resource constraints (Brush et al., 2011 [1]). In parallel, researchers have been working on designing hardware and software solutions to address these challenges, leading to notable progress in developing secure and efficient smart doors (Capogrosso et al., 2022 [2]; Eze et al., 2023 [3]).

Despite this progress, there remain open questions about how to simultaneously ensure robust security, maintain low latency, and offer personalized interactions without overburdening network or cloud resources. Traditional smart door lock systems often rely on cloud-based services for tasks such as identity recognition and voice command processing (Hadis & Aman, 2020 [4]). While these services can be powerful, dependence on external servers raises concerns related to data privacy, reliability, and the need for constant internet connectivity (Kaaz et al., 2017 [6]). Such concerns underscore the importance of local computation and on-device intelligence.

One promising approach to achieving on-device intelligence involves the use of Small Language Models (SLMs), which strike a balance between advanced natural language

understanding and resource efficiency (Robinson, 2024 [24]). In contrast to Large Language Models (LLMs) that typically require substantial computational resources and external cloud infrastructures, SLMs can operate under more constrained conditions, making them well-suited for real-time applications in embedded systems (Splunk, 2024 [25]). Recent developments further highlight how SLMs can be specialized to specific domains, thereby reducing latency and bandwidth demands while still providing accurate language processing and decision-making capabilities (Kwon et al., 2024 [23]; Yao et al., 2024 [21]).

Building on these insights, this paper introduces a multi-agent architecture for smart door automation that integrates SLMs to address critical tasks such as user identification, access control, and interactive response generation. By distributing computational responsibilities among multiple specialized agents—ranging from door control to biometric recognition—our framework aims to reduce single points of failure, improve reliability, and allow real-time response. The Identity Recognition Agent employs lightweight vision-based methods such as You Only Look Once (YOLO) to distinguish between family, friends, and unknown visitors (Capogrosso et al., 2022 [2]; Ishrat et al., 2017 [5]), while the Response Management and Audio Response Agents leverage SLMs to parse and generate voice-based interactions on the fly. This setup prioritizes privacy by performing critical processing on local hardware, mitigating the risks associated with sending user data to external servers.

Initial tests reveal that our multi-agent, SLM-based approach supports strong security controls, personalized user interactions, and easy expansion for different home settings. The upcoming sections break down each system component, explain the main technologies and methods, and present results that highlight the strengths of this design. Lastly, we summarize the key advantages, note potential drawbacks, and suggest directions for continued development in smart door automation.

2. Literature Review

Smart door automation has long been influenced by broader studies of home automation, where researchers have grappled with how best to integrate technology into people's everyday routines. Early investigations recognized that door systems lie at the heart of household security and convenience, yet also pose unique privacy and usability challenges. Brush et al. (2011) [1], for example, underscored the variety of user needs and technical hurdles encountered when automating household tasks, while Woodruff, Augustin, and Foucault (2007) [9] highlighted how cultural and religious contexts can deeply affect the design and adoption of home automation solutions. These foundational findings paved the way for more specialized work focusing on doors specifically, an area in which robust hardware, seamless user experience, and adaptive security protocols converge.

As researchers turned their attention to smart door systems, several studies began incorporating advanced sensors, connectivity modules, and integrated software in pursuit of safer and more convenient entry mechanisms. Capogrosso et al. (2022) [2] elaborated on the promise of a future where networked doors, equipped with sophisticated sensing abilities, ease daily routines and strengthen overall home security. Meanwhile, Eze et al. (2023) [3] expanded on this notion by examining how hybrid door control methods, combining traditional locks with digital authentication, can enhance both reliability and user satisfaction. However, these innovations also exposed potential security gaps. Kaaz et al. (2017) [6] pinpointed several common flaws in smart lock systems, illustrating how insufficient encryption and outdated protocols can leave even highly connected homes vulnerable to intrusion. Efforts to address these vulnerabilities often focus on balancing airtight security with the practical needs of everyday users. Hadis and Aman (2020) [4] investigated various wireless access approaches, revealing that while stronger encryption methods bolster protection, they may also hinder tasks requiring near-instantaneous response times such as unlocking doors in an emergency. Other researchers, including Verma and Tripathi (2010) [8] and Zedig (2022) [10], examined RFID-based access and broader architectural weak points, emphasizing that the convenience offered by cutting-edge systems must never overshadow the need for comprehensive defense against unauthorized access.

In parallel, many studies turned to artificial intelligence to refine the way doors detect and respond to potential entrants. Ishrat et al. (2017) [5] demonstrated that even resource-constrained hardware can implement machine learning algorithms to improve authentication accuracy. Sutikno et al. (2024) [7] extended this idea by combining microcontroller platforms, like Arduino, with biometric sensors, creating flexible setups capable of verifying users in real time. Yet a common thread in these AI-driven methods was a reliance on cloud-based services for tasks such as speech recognition or data processing (Hadis & Aman, 2020 [4]), a dependence that can create bottlenecks, generate privacy concerns, and raise latency issues.

In response, Small Language Models (SLMs) have emerged as a compelling solution for on-device intelligence. Unlike Large Language Models (LLMs) that demand robust hardware or cloud computing to operate effectively, SLMs demonstrate sufficient accuracy in interpreting commands and delivering responses while reducing latency and bandwidth requirements (Robinson, 2024 [24]; Splunk, 2024 [25]). Kwon et al. (2024) [23] and Yao et al. (2024) [21] further championed SLMs for their enhanced privacy protections, noting that minimal cloud interaction inherently limits the exposure of sensitive data. This development opens up new pathways for integrating SLMs into smart door automation, particularly in scenarios were system responsiveness and data security carry utmost importance.

Despite these promising directions, there is still a need for an overarching framework that unites strong security, adaptive AI capabilities, and an intuitive user experience. Much of the existing research has focused either on technical security measures, hardware improvements, or standalone AI techniques, without fully merging these aspects into one comprehensive system. The approach presented in this paper aims to fill this gap by introducing a multi-agent design that leverages SLMs to ensure secure, efficient, and personalized door access. This solution builds directly on the foundations laid out in prior studies, yet strives to integrate them into a unified system poised to address the key challenges of modern smart door automation.

3. Methodology

In this research, we propose a Multi-Agent Smart Door Management System using Small Language Models (SLMs) to facilitate real-time automation, security, and user interaction. Unlike traditional sequential agent systems, we adopt a parallel multi-agent approach, enabling concurrent task processing. This design ensures faster response times and more robust decision-making

Let $A = \{a_1, a_2, \dots, a_n\}$ represent the set of n agents (here, $= 5$). Each agent a_i has a state space S_i, an action set Act_i, and a transition function δ_i. The system follows an event-driven model, where every agent reacts asynchronously to incoming requests and signals.

$$T_{sys} = max_{a_i \epsilon A}(T_{a_i}) \quad \text{....(1)}$$

Equation (1**)** expresses the overall system response time T_{sys}. Since agents operate in parallel, the total completion time depends on the maximum of individual agent execution times T_{a_i}, rather than their sum. This parallelism markedly reduces latency compared to sequential pipelines.

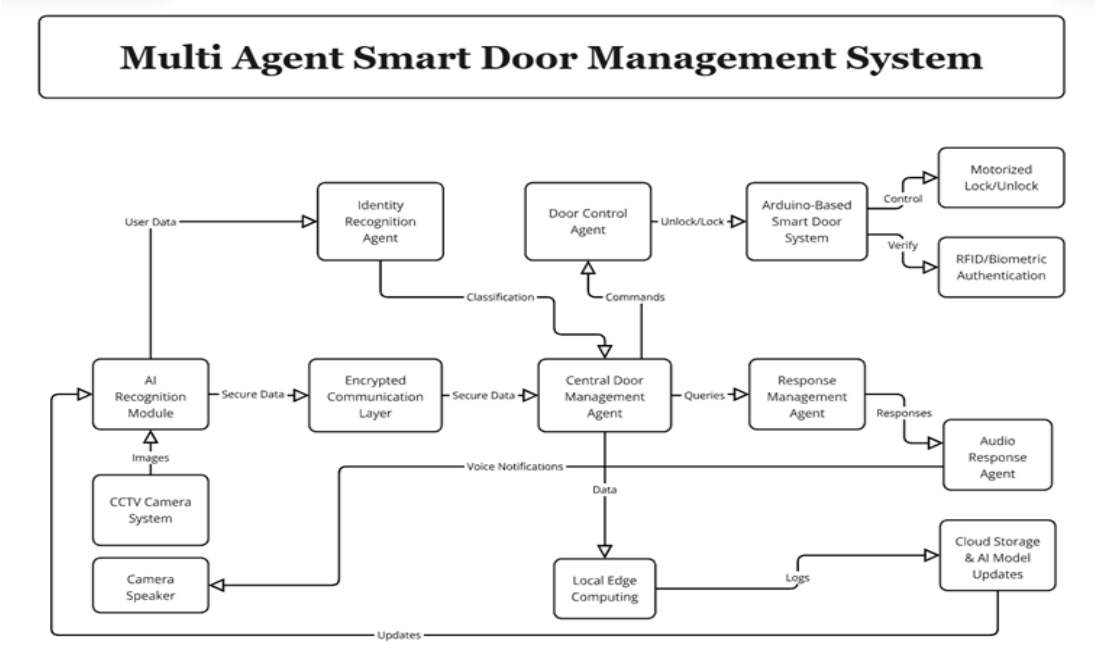

Fig.1: Smart Door System with AI, Arduino, and SLM Agents for Security and Automation.

As shown in Figure 1, the Multi-Agent Smart Door Management System is designed to facilitate seamless coordination among various agents operating in parallel. The diagram illustrates the dynamic interactions between the Central Door Management Agent (CDMA), Response Management Agent (RMA), Door Control Agent (DCA), Identity Recognition Agent (IRA), and Audio Response Agent (ARA). Each agent processes specific tasks concurrently, optimizing efficiency and reducing latency. The directional arrows in the figure represent real-time data exchange and event-triggered communication, ensuring a streamlined and intelligent door management system.

To achieve parallel functioning, each agent operates asynchronously, subscribing to a centralized event-driven message queue. This queue ensures real-time updates and coordination among agents. The system uses multi-threading and non-blocking communication protocols to prevent latency bottlenecks. Each agent processes incoming requests independently, leveraging lightweight SLMs to maintain efficiency. The framework supports concurrent execution of identity verification, response generation, and door control actions without unnecessary dependencies. The diagram illustrates the dynamic interactions between the Central Door Management Agent (CDMA), Response Management Agent (RMA), Door Control Agent (DCA), Identity Recognition Agent (IRA), and Audio Response Agent (ARA). Each agent processes specific tasks concurrently, optimizing efficiency and reducing latency. The directional arrows in the figure represent real-time data exchange and event-triggered communication, ensuring a streamlined and intelligent door management system.

4. Performance Analysis of System Modules

4.1.1 Central Door Management Agent (CDMA)

- Central coordinator for all agent interactions.
- The CDMA ensures seamless communication using event-driven architecture and message queuing, allowing real-time coordination.
- Transition Function (δ_{CDMA}): Receives event e, updates its internal state, and broadcasts relevant instructions to other agents.
- Implements concurrency protocols to manage parallel requests, ensuring no single agent creates a bottleneck.

4.1.2 Response Management Agent (RMA)

- Processes authentication decisions and generates appropriate responses efficiently.
- Defines a response decision function $f_{RMA}(x)$, where x includes visitor identity. Secuirity status, and other contextual variables.

$$f_{RMA}(x) = \begin{cases} 1, & if\ authorized\ and\ no\ threat\ detected, \\ 0, & otherwise. \end{cases}$$

- Operates independently, listening for updates from the Identity Recognition Agent (IRA) and user requests from the Audio Response Agent (ARA).
- Using adaptive learning mechanisms to enhance response accuracy over time.

4.1.3 Door Control Agent (DCA)

- Manages the physical door operations of locking and unlocking via IoT devices (e.g., an Arduino-based system).
- Employs a real-time control function $\alpha_{DCA} = g(\theta, \phi)$, where θ and ϕ are indicators of door status and authorization signals.
- Runs as a parallel thread, enabling immediate door action upon receiving authorization.
- Using safety mechanisms to handle hardware malfunctions.

4.1.4 Identity Recognition Agent (IRA)

- Provides accurate identity verification using multi-modal biometric authentication.
- Uses YOLOv8 for facial recognition, supplemented by RFID and biometric validation.
- Uses a weighted formula $C_{IRA} = \alpha \cdot p_{face} + \beta \cdot p_{RFID} + \gamma \cdot p_{bio,}$ where $\alpha + \beta + \gamma = 1$. If $C_{IRA} \geq \tau$, the user is deemed authorized.
- Operates continuously to preemptively verify individuals, minimizing wait times for authentication.

4.1.5 Audio Response Agent (ARA)

- Generates voice-based interactions and alerts using text-to-speech (TTS).
- SLM-Driven Interaction: Uses a lightweight language model to interpret contextual cues (e.g., visitor ID, user instructions) and produce natural language responses.
- Using low-latency SLM and text-to-speech (TTS) models to generate seemless customized responses.
- Concurrency Model: Functions alongside IRA and RMA, ensuring prompt feedback for visitors (e.g., greetings, door-status announcements).

4.2 Efficiency & Scalability

- Parallel execution minimizes latency, ensuring rapid agent responses.
- Asynchronous messaging enables uninterrupted operation and avoids agent blocking.
- Scalability is achieved by integrating additional agents for extended functionalities such as advanced anomaly detection.

4.3 Security & Reliability

- Multi-layer authentication enhances security by combining biometric, RFID, and facial recognition.
- Safety mechanisms allow system recovery in case of partial failures.
- Audit logs provide real-time security monitoring and event tracking.

4.4 User Experience

- Instant authentication ensures smooth and frictionless access control.
- Adaptive identity recognition improves system responsiveness and accuracy.
- Real-time audio feedback enhances user interaction and acces

4.5 Challenges & Future Improvements

- Computational overhead requires optimized resource allocation for efficiency.
- Security vulnerabilities in wireless transmissions necessitate advanced encryption strategies.
- Future updates include AI-based anomaly detection and blockchain-secured event logging.

5. Conclusion

The Multi-Agent Smart Door Management System enhances security, efficiency, and user experience by leveraging SLMs, YOLOv8-based recognition, and event-driven multi-agent coordination into a seamless access management solution. The ability to process multiple authentication requests in parallel reduces response times, optimizes scalability for larger infrastructures, and continuously refines recognition accuracy through AI-driven models that adapt to dynamic access patterns. Multi-factor authentication adds an additional layer of protection, significantly minimizing security risks. Future advancements will focus on AI-driven threat prediction, real-time failure detection, and greater smart home integration to ensure seamless interoperability. Furthermore, the system incorporates intelligent workload balancing to efficiently manage fluctuating authentication requests during peak times, preserving performance and stability. Adaptive thresholding dynamically adjusts identity verification criteria based on real-time security conditions, enhancing both accessibility and protection. The real-time analytics dashboard offers comprehensive insights into access trends, enabling administrators to proactively refine security protocols. This holistic approach establishes a highly adaptive, intelligent security ecosystem designed to meet evolving access management demands with precision, agility, and resilience against emerging threats.

References

1. Brush, A. J. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., & Dixon, C. (2011). Home automation in the wild: Challenges and opportunities. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2115–2124. https://doi.org/10.1145/1978942.1979249
2. Capogrosso, L., Skenderi, G., Girella, F., Fummi, F., & Cristani, M. (2022). Toward smart doors: A position paper. arXiv preprint arXiv:2209.11770.
3. Eze, V. H. U., Edozie, E., & Jama, I. M. (2023). Automated hybrid smart door control system. IAA Journal of Scientific Research, 10(1), 36–48.
4. Hadis, S., & Aman, F. (2020). A survey on smart door lock security methodologies implemented using various wireless access technologies. International Research Journal of Modernization in Engineering Technology and Science, 2(9), 1814–1818.
5. Ishrat, I., Ali, W. M., Ghani, S., Sami, S., Waqas, M., & Aftab, F. (2017). Smart door lock system with automation and security. Science International, 29(1), 73–76.
6. Kaaz, K. J., Hoffer, A., Saeidi, M., Sarma, A., & Bobba, R. B. (2017). Security in smart locks. 2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC), 297–301.
7. Sutikno, T., Ubaidillah, M. A. F., Arsadiando, W., & Purnama, H. S. (2024). Fingerprint-based smart door

lock system using Arduino and smartphone application. Computer Science and Information Technologies, 1(1), 1–7.
8. Verma, G., & Tripathi, P. (2010). A digital security system with door lock system using RFID technology. International Journal of Computer Applications, 5(11), 6–8.
9. Woodruff, A., Augustin, S., & Foucault, B. (2007). Sabbath day home automation: "It's like mixing technology and religion". Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 527–536. https://doi.org/10.1145/1240624.1240710
10. Zedig, J. (2022). Security in smart locks. Bachelor's thesis, Blekinge Institute of Technology.
11. 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.
12. 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.
13. Yellapragada, S., Li, Z., Doshi, K. B., Mhasakar, P. M., Fan, H., Wei, J., Blasch, E., Zhang, B., & Ling, H. (2023). CCTV-Gun: Benchmarking handgun detection in CCTV images. arXiv preprint arXiv:2303.10703.
14. 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.
15. 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.
16. 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.
17. Yellapragada, S., Li, Z., Doshi, K. B., Mhasakar, P. M., Fan, H., Wei, J., Blasch, E., Zhang, B., & Ling, H. (2023). CCTV-Gun: Benchmarking handgun detection in CCTV images. arXiv preprint arXiv:2303.10703.
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). 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
44. 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. (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
47. 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
48. 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
49. 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
50. 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
51. 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
52. 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
53. 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
54. 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
55. 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
56. 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
57. 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
58. 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
59. 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
60. 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