Towards a Smarter Workplace: IOT-Enabled Intelligent Office Appliances

Yassir Farooqui[1], Walter Alisio[2], Aung Kyaw Hein[3], Emmanuel Johannes Ngemera[4], Chetanya Singh[5]
Department of Computer Science and Engineering
Parul Institute of Engineering and Technology, Vadodara, Gujarat, India
{yassir.farooqui270062, 2203031050811, 2203031050070, 2203031050183, 2203031050135}@paruluniversity.ac.in

***Abstract*—The demand for smart and efficient workplace solutions has led to a significant boom in the smart office automation industry. Traditional methods, like manual switching and controlling appliances separately, often don't cut it when it comes to efficiency, personalization, and user satisfaction. That's where Smart Office Appliances with IoT comes in, aiming to transform this space with a user-friendly web application that streamlines the whole automation process. The application boasts features such as dynamic appliance monitoring, personalized automation, secure online communication, real-time control, and flexible energy management. By harnessing the latest in IoT technologies and combining them with office appliances, this solution enhances accessibility, improves the user experience, and boosts workplace efficiency. It strives to bridge the gap between traditional office setups and the convenience of digital solutions, offering a seamless and reliable option for anyone looking to create a smart, connected, and automated work environment.**

***Index Terms*—IoT, smart office, automation, real-time control, energy management**

I. Introduction

The voluminous expansion of intelligent devices, fueled by fifth-generation (5G) networks and cloud computing, has transformed the way office spaces operate. This revolution enabled the operation of Internet of Things (IoT) applications in priority areas such as smart cities, energy management, healthcare, transportation, and office automation [1,2,17]. IoT combines sensors, communication protocols, and data analysis to enable smart systems with the ability to sense, analyze, and respond to real-time conditions immediately [3]. In offices, this combination has given rise to the concept of the smart office, where connectivity and automation enhance resources, comfort, and productivity [7,8].

Smart offices employ IoT-driven communication among sensors, actuators, and technologies. These involve device-to-device (D2D), machine-to-machine (M2M), and machine-to-human (M2H) communications [20,21,23]. These systems assist in the control and monitoring of basic building services such as lighting, ventilation, heating, and air quality. For instance, intelligent systems are able to modify lighting and airflow according to occupancy characteristics, indoor conditions, and individual preferences and decrease energy consumption while sustaining comfort [14,15]. Artificial intelligence (AI) also enables early detection of office system issues through predictive maintenance. This enhances reliability, minimizes downtime, and guards against employee health [16,26,27]. All these capabilities transform conventional office environments into intelligent offices by infusing wisdom into routine workplace operations.

Cloud and edge computing together increase the efficiency of smart offices even more. Cloud platforms provide elastic storage, sophisticated data analysis, and customized services, and edge computing enables real-time, rapid processing of data near the site of data collection [18,21]. This hybrid arrangement caters to scalability and privacy issues, making smart office applications operate smoothly and safely. High-end wireless networks support real-time operations such as access control, intrusion detection, alarm systems, and workspace personalization, enhancing the capabilities of intelligent office spaces [4,9]. Such technologies also facilitate global sustainability goals, as continuous IoT monitoring has demonstrated significant improvements in energy efficiency, infrastructure utilization, and environmental sustainability in commercial buildings and campuses [5,6,19].

But beyond technology lies the growth of intelligent offices based on human factors. Studies reveal that user experience, comfort, personalization, and perception of health effects are essential for adoption and success [11]. Workers today assume that technologies will make work easier to perform while promoting wellness by reducing stress, optimizing energy consumption, and designing healthier workplaces. With all these advances still present, issues persist, particularly surrounding cybersecurity, privacy, and system compatibility. Issues such as ownership of data, surveillance, and balancing convenience and privacy deter wholesale adoption [12,30]. Future office designs must be human-centric with a focus on transparency, trust, and inclusivity and with robust security and interoperability.

Finally, the convergence of IoT, 5G, and cloud-edge computing in the workplace holds tremendous promise for creating responsive, sustainable, and secure workplaces. By integrating technological innovation with sustainability and human-centered design, smart offices have the potential to increase operational efficiency, energy consumption, productivity, security, and employee health. Yet, scalability, globalization compatibility standards, and ethical challenges remain. Thus, smart offices that are IoT-based offer a new ground on which information and communication technologies, human values, and sustainability converge and symbolize an important step toward future intelligent offices [22,25,28,29].

II. Literature Review

Yung Po Stang et al. [2] introduced a new system that integrates blockchain with IoT technologies to develop a food traceability system. Their Blockchain-based IoT Food Traceability System (BIFTS) controls perishable items' shelf life using lightweight blockchain attributes and certain consensus method. This method takes into account shipment transit duration, stakeholder assessment, and shipment quantity, enhancing transparency and trust within the supply chain.

Likewise, Agrawal et al. [3] researched blockchain solutions in supply chain management (SCM), a critical role that regulates the supply of goods and services between stakeholders. Their overview provided insights into uses of blockchain, functional attributes, and effects on various SCM cycles. Moreover, Nasir et al. [4] wrote on the significance of secure IoT-based systems in enhancing SCM. They proposed an IoT-based reporting and monitoring framework that can real-time update the quality of perishables, providing safety, reliability, and efficiency.

Oscar Nova et al. [9] looked into the underlying consensus algorithms within blockchain and how they impact decentralized systems. They presented some blockchain models and compared the roles and capabilities of IoT within such systems. Jaime Chan et al. [10] furthered this research by proposing a blockchain-based access control system. Their design, proven using a proof-of-concept prototype, demonstrated that decentralized identity management in IoT devices is possible.

Yu Chen et al. [11] extended this research towards emphasizing access control in IoT settings. They asserted that existing Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) strategies fall short in the scalability and adaptability requirements of IoT networks. To address this, they developed an access control system based on blockchain and implemented it on a private blockchain using resource-limited devices such as Raspberry Pi, showing its applicability in actual IoT systems.

III. Objectives

To foster an intelligent, sustainable, secure, and employee-centric workspace through the integration of connected devices, sensors, and data analytics into daily operations.

Key Benefits: Enhanced Energy Efficiency and Sustainability: The intelligent management of appliances (lighting, AC, computers) based on occupancy, environmental conditions, and real-time usage leads to reduced energy waste, lower operational costs, and the promotion of eco-friendly practices, thereby helping to achieve corporate sustainability goals. Improved Security and Safety: By integrating with RFID access systems, surveillance cameras, and environmental sensors (gas, smoke, and fire detectors), a robust security infrastructure is built. Real-time monitoring and automated alerts safeguard both employees and assets. Optimized Comfort and Productivity: Automating appliances to maintain ideal lighting, temperature, and air quality creates a healthier and more comfortable work environment, supporting employee well-being and boosting overall productivity. Reduced Manual Intervention: Routine appliance management is automated, minimizing human effort and offering flexibility through re- mote access via mobile or web applications. Data-Driven Facility Management: Continuous data collection on appliance usage and occupancy patterns provides actionable insights for predictive maintenance and optimized space utilization.

IV. System Design

The Smart Office Appliances with IoT System has a modular and full-stack architecture. This system integrates IoT devices, cloud computing, and web platforms to produce a user-friendly smart office experience. Its creation has a straightforward process involving requirement gathering, system designing, technology selection, solution implementation, extensive testing, and final product deployment. This makes it reliable and robust. This approach enables expansion and rapid adaptation while it is simple to introduce new features and devices in the future. The platform prioritizes good system performance, security, and user experience, resulting in high user interaction and simple office management that produces an intelligent and adaptable working environment.

The system incorporates real-time data analysis to provide useful insights for maintenance forecasting, resource utilization, and energy efficiency. It facilitates collaboration across disparate devices, enabling sensors, smart devices, and management platforms to collaborate seamlessly. The cloud-based architecture enables remote access, allowing users to control and monitor office spaces remotely from anywhere, anytime. Robust security features, including encryption and role-based access control, safeguard sensitive business data against cyber attacks. Overall, this integrated system transforms ordinary offices into smart, active, and future-proof workplaces.

V. METHODOLOGY

Figure 1 illustrates a web application system structure with a Node/Express backend and a React frontend. The User begins with the User Browser, which interacts with the React Frontend App. Users proceed to the Login Page or the Signup Page. Upon login or signup, the app sends POST requests to the backend URLs: /api/auth/login for login or /api/auth/signup for signup. The AuthContext is responsible for the results of these calls. It is responsible for the authentication state, which involves the token, the user, and the logged-in state. The JSON Web Token (JWT), received upon successful login or registration, is saved in the browser's localStorage for continuous authentication. This arrangement allows users to access Protected Routes, such as device and sensor pages, that require the correct authentication. These routes terminate on the Backend API constructed using Node/Express, which serves multiple endpoints like /api/auth/login, /api/auth/signup, /api/devices, and /api/sensors.

The system ensures secure access and seamless interaction between the backend and frontend. As the system does not maintain heavy server-side sessions and relies on JWTs, it is lightweight and scalable. The secure paths involve role-based or token-based authentication, preventing unauthorized users from accessing sensitive device and sensor information. React Context provides a single point of control to handle authentication in the application, and it is simpler compared to working with prop drilling. Express handles routing and API calls on the server side and serves as a bridge between the frontend and the database or other services. It is simple to add on to the module-based API endpoints, like adding more types of devices or sensor capabilities in the future.

The backend API also interfaces with a database layer such as MongoDB or SQL, where user passwords, device data, and sensor data are securely stored and retrieved. During authentication, the backend verifies user passwords against the database before sending out a JWT. Equally, when users request device or sensor data, the API retrieves data from the database and passes it to the frontend. Encryption and hashing algorithms, such as bcrypt for passwords, are utilized to provide user security. Indexing and query optimization methods enable the application to scale with an increase in the number of devices and users. This database integration rounds off the architecture to ensure permanent storage, reliability, and integrity of data.

This design also promotes reusability and modularity because each component (frontend, backend, and database) can be independently upgraded without affecting the whole system. Usage of JWTs also makes the system stateless, which is beneficial for being deployed on multiple servers or cloud configurations. Separating the concerns between UI, authentication, and data handling makes the system simpler to maintain and scale. Generally, this architecture is a good compromise between usability, security, performance, and scalability and thus is well-suited for IoT device management and real-time sensor monitoring applications.

VI. System Architecture

Figure 2 illustrates how a web application functions from startup through authentication, route protection, and device and sensor interaction.

The process begins with Start App, which starts the application with Server.js. The application then splits into two primary domains. On one end, Shared UI Components such as Navbar.js, Footer.js, and api.js provide shared frontend functionality that is reused throughout the app. These components connect to Signup.js, where new users register through a POST /api/auth/signup request. On the other side, AuthContext.js handles the authentication state, including user details, login status, and tokens. This works with ProtectedRoute.js, which makes sure that only authenticated users can access restricted routes like the devices and sensor pages.

If a user registers or logs in using Login.js (POST
/api/auth/login), the backend verifies the credentials with the database (such as MongoDB or SQL). If the credentials are right, the backend generates a JWT (JSON Web Token) and returns it to the frontend. The token is then stored within the browser (such as localStorage) and can be used on subsequent requests. The Authenticated? step verifies whether there is a verified token by the backend. If authentication fails, the process is directed back to the login step. If successful, the user proceeds to Dashboard.js, which now serves as the central hub of authenticated interactions.

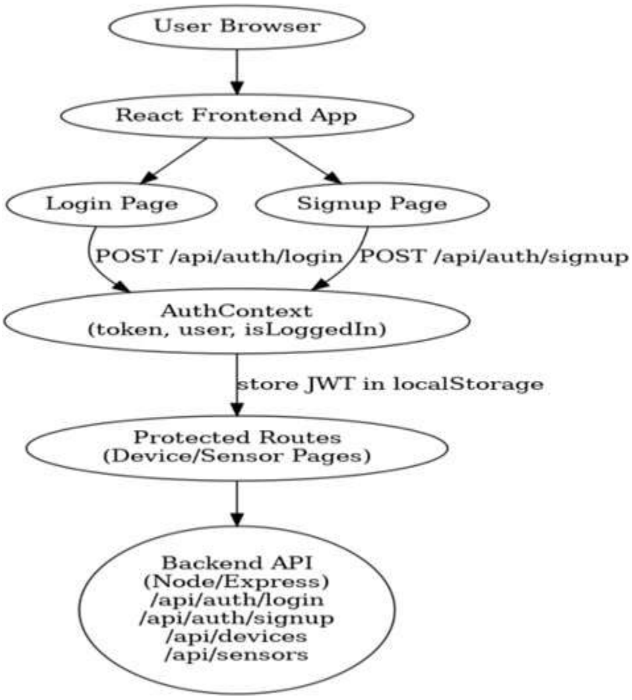

Fig. 1. The mechanism from user end

From the dashboard, users can Logout, which cleans the AuthContext, deletes the JWT, and routes them back to login. Or, they may see devices using Devices.js, which makes a GET /api/devices request to the backend. The backend validates the JWT before fetching the device data from the database and passing it along to the frontend. Sensors.js makes a GET /api/sensors request to retrieve real-time or cached sensor data, similarly protected by JWT validation. In the device management section, users are allowed to add new devices using AddDevice.js that sends a POST /api/devices request to the backend. Backend validates the JWT, stores the new device in the database, and refreshes the device list.

The utilization of JWTs makes each request to safeguarded routes secure and associated with a valid session without the use of server-side session storage, which is heavy. The user accounts, devices, and sensor data are stored in the database layer. Password storage employs hashing (such as bcrypt), and queries are optimized for scaling with growth as the system grows. This design establishes a secure, modular, and scalable system for authentication, devices, and sensor data handling.

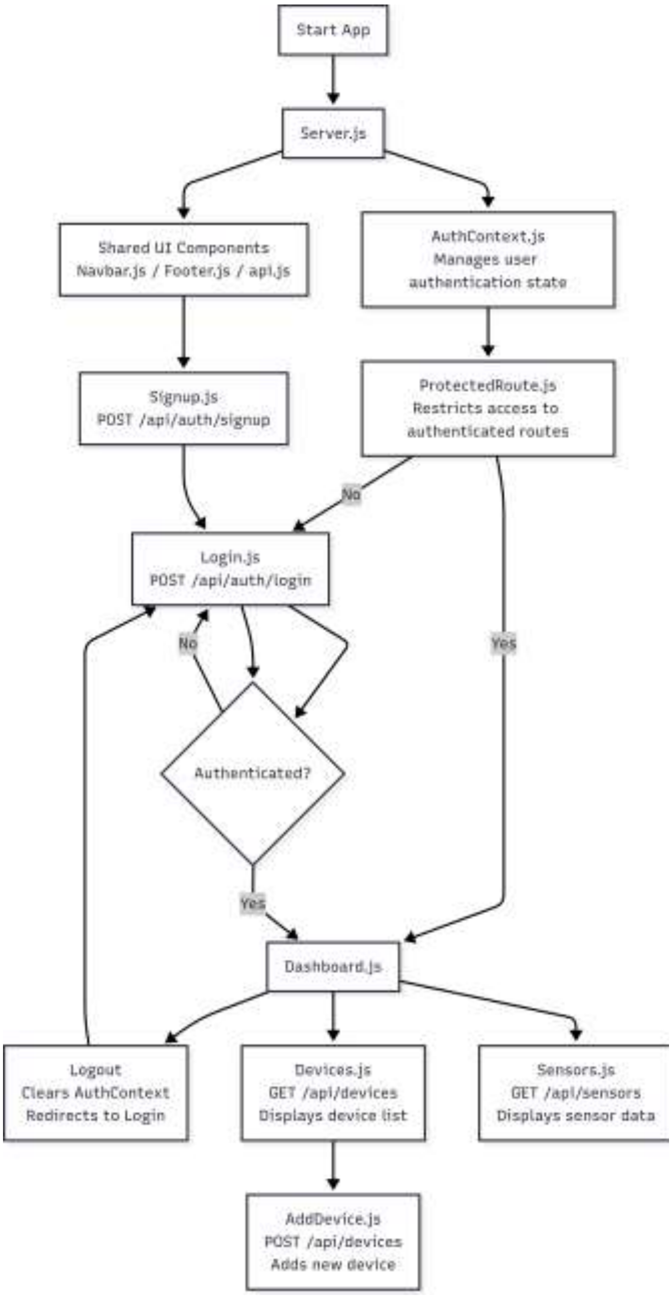

Fig. 2. System Architecture

VII. Results

The IoT Home Appliances Application aims to bridge the gap between users and smart home devices, focusing on convenience, personalization, and reliability. This system caters to residents, working professionals, and administrators by offering real-time appliance monitoring via integrated IoT protocols, flexible automation scheduling, and subscription-based services that simplify daily tasks.

Users benefit from an intuitive admin dashboard, which streamlines appliance management, task scheduling, and performance tracking. The platform's modular design ensures seamless scalability and updates. To safeguard user data and transactions, robust security measures are implemented, including password hashing, token-based authentication, and encrypted communication.

During testing, minor technical issues were promptly addressed through optimization. User feedback also guided further enhancements, such as analytics for energy consumption, push notifications, and a dedicated mobile application for improved accessibility. Ultimately, this platform harmonizes traditional appliance use with digital innovation, simplifying users' lives and empowering households within the expanding IoT ecosystem.

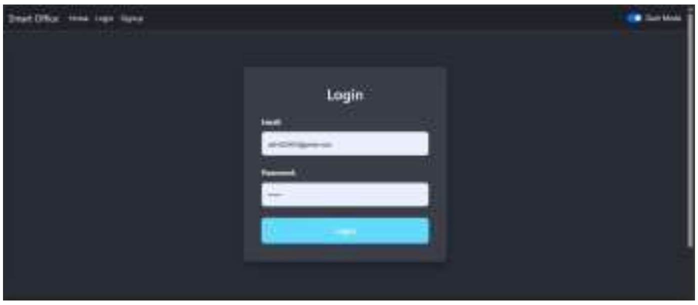

Fig. 3. User Sign Up/Log In Interface

In figure 3, the Smart Office system focuses on security with its login screen, which requires users to enter their registered email and password. This important step verifies that only authorized users can access smart devices, view sensor data, and change system settings. By confirming user credentials, the system stops unauthorized access and protects sensitive information related to office operations and employee activities.

In addition to basic authentication, the login process can include features like password recovery, multi-factor authentication, and role-based access control. These features improve security by making sure different user levels—such as administrators, employees, and guests—have the right permissions. This layered approach keeps operations running smoothly while maintaining the integrity of the smart office environment.

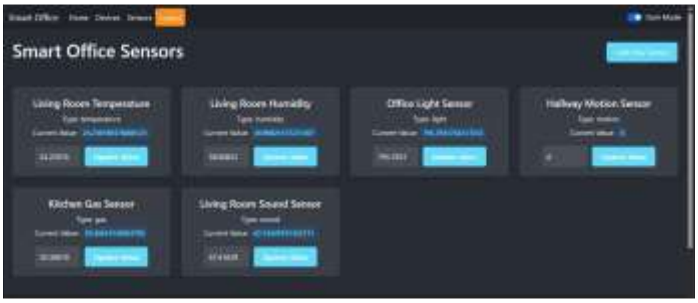

Fig. 4. Sensors Interface

In figure 4, the interface gives a clear overview of the smart office environment. It uses integrated IoT sensors to provide real-time data on temperature, humidity, light, gas, sound, and motion. By continuously tracking these factors, the system helps understand the office's environmental conditions. This supports quick decision-making.

In addition to automatic updates, users can manually refresh or change sensor readings. This adds accuracy and flexibility to monitoring. The collected data not only improves comfort and safety but also plays a key role in automation. For example, it can adjust lighting based on brightness or send alerts for gas leaks or unusual motion.

This smooth integration of IoT sensors allows for efficient monitoring, proactive safety measures, and better resource management. It ultimately promotes a smarter, safer, and more sustainable office environment.

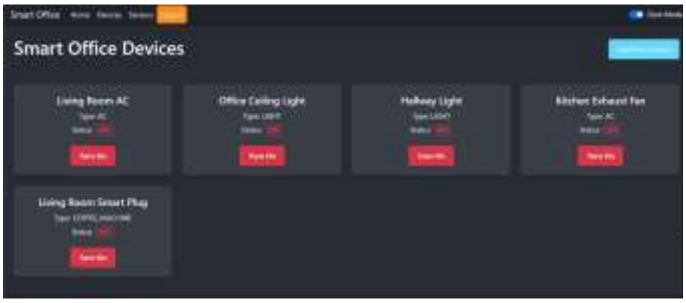

Fig. 5. Devices Interface

In Figure 4, the interface gives a clear view of the smart office environment. It uses integrated IoT sensors to provide real-time data on temperature, humidity, light, gas, sound, and motion. By continuously monitoring these factors, the system helps users understand the office's environmental conditions, allowing for timely decision-making.

Users can manually refresh or adjust sensor readings to ensure accuracy and flexibility in monitoring. The data collected improves comfort and safety and plays a key role in automation. For example, it can adjust lighting based on brightness or send alerts for gas leaks or unusual movement. This integration of IoT sensors enables efficient monitoring,

proactive safety measures, and better resource management. It ultimately creates a smarter, safer, and more sustainable office environment. In Figure 5, the office's smart device control panel serves as a hub for managing essential appliances like the AC, lights, exhaust fan, and smart plug. It allows for remote operation, giving the user the ability to easily turn devices on or off, either manually through the interface or automatically based on pre-set conditions. The panel also provides real-time status updates for all connected devices, keeping users informed about which systems are active or inactive.

In addition to basic switching, the panel supports automation and energy savings by connecting to sensors that detect occupancy, temperature, and light levels. For instance, lights can automatically turn off when a room is empty, or the AC can adjust to maintain comfort while reducing power use.

This functionality shows how IoT helps with centralized device management, offering convenience, better energy efficiency, and less manual work. The system's ability to grow allows for future integration of more smart devices, creating a flexible and adaptable office environment that encourages operational efficiency and sustainability.

Fig. 6. User Credentials in Database

In figure 6, the MongoDB database for the Smart Office system stores user data. Each user record includes a unique identifier (id), email address, and a securely hashed password. Bcrypt hashing protects sensitive data. It ensures secure authentication and prevents unauthorized access.

In addition to these basic fields, the design can include role-based access, such as admin or employee, and activity logs for flexible user management. This setup not only protects personal information but also creates a scalable basis for effective authentication and authorization within the Smart Office system.

VIII. Future Works

The IoT Home Appliances Application is set for significant enhancements to boost its functionality, user convenience, and intelligence. A key development is the introduction of a dedicated mobile app for both Android and iOS, providing users with seamless remote monitoring and control of their appliances. An AI-powered recommendation system will personalize appliance operation, optimizing energy use and comfort based on user behavior, routines, and preferences.

To ensure inclusivity, the platform will offer multi-language support. A new maintenance partner module will simplify coordination with service providers, offering real-time updates on repairs. Users will also gain access to detailed energy consumption insights and a power usage tracker, enabling data-driven decisions for smarter appliance management.

Future updates include an AI-driven chatbot for instant support and a smart feedback analysis system to continually improve appliance management through user reviews. These collective advancements aim to establish the platform as a comprehensive, intelligent, and scalable IoT-based home automation solution, transforming traditional homes into fully connected, efficient, and user-centric smart environments.

- Dedicated mobile apps (Android/iOS).

- AI-powered appliance recommendation system.
- Multi-language support.
- Separate maintenance partner module.
- Energy analytics and power usage tracker.
- AI chatbot and smart feedback system.

IX. Conclusion

The IoT Home Appliances Application signifies a considerable leap in household management, transitioning from manual interaction to an intelligent, automated, and secure digital framework. This innovation not only elevates daily ease but also champions global sustainability through effective energy management. Its intuitive interface, featuring real-time monitoring, customizable automation, and adaptable scheduling, guarantees a fluid user experience.

Beyond individual residences, this platform presents opportunities for communal living areas, rental properties, and residential complexes. It enables centralized yet personalized appliance control, leading to reduced energy expenditures and enhanced living standards. Robust security measures further foster confidence, establishing it as a dependable solution for contemporary living.

Forthcoming enhancements include mobile app integration, AI-driven predictive recommendations, cloud synchronization, and voice-assistant compatibility, establishing a flexible foundation prepared to accommodate evolving user demands.

In essence, the IoT Home Appliances Application is set to transform household management by consolidating convenience, efficiency, and sustainability within a unified digital ecosystem. Its foundational principles of simplicity, dependability, and continuous innovation position it as a cornerstone for the future of smart living.

Acknowledgment

I extend my sincere gratitude to Mr. Yassir Farooqui, Assistant Professor, for his invaluable guidance and unwavering encouragement throughout this project. I am also thankful to the Head of the Department, faculty, and staff of the Computer Science and Engineering Department for providing essential resources and fostering a supportive academic environment. My heartfelt appreciation goes to my teammates and peers for their cooperation and constructive feedback. Finally, I thank my family for their unwavering love and moral support, and everyone else who contributed, directly or indirectly, to the successful completion of this project.

References

[1] Chettri, L., & Bera, R. (2019). A comprehensive survey on IoT toward 5G wireless systems. IEEE IoT Journal, 7(1), 16–32.

[2] Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1–9.

[3] Alfa, A. S., Maharaj, B. T., Ghazaleh, H. A., & Awoyemi, B. (2018). The role of 5G and IoT in smart cities. In Handbook of Smart Cities (pp. 31–54).

[4] Gaba, G. S., Kumar, G., Kim, T.-H., Monga, H., & Kumar, P. (2021). Se- cure device-to-device communications for 5G-enabled IoT applications. Computer Communications, 169, 114–128.

[5] Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019). Smart cities: Advances in research—An information systems perspec- tive. International Journal of Information Management, 47, 88–100.

[6] Mishra, P., Thakur, P., & Singh, G. (2022). Sustainable Smart City to Society 5.0: State-of-the-Art and Research Challenges. SAIEE Africa Research Journal, 113(4), 152–164.

[7] Kumar, A., Kumar, P. S., & Agarwal, R. (2019). A Face Recognition Method in the IoT for Security Appliances in Smart Homes, Offices, and Cities. In Proc. ICCMC 2019 (pp. 964–967).

[8] Jion, M. S. A., & Ahmad, M. (2024). A Smart and Secured Office System Using IoT. In Proc. iCACCESS 2024 (pp. 1–7). IEEE.

[9] Painuly, S., Sharma, S., & Matta, P. (2021). Future trends and challenges in next generation smart application of 5G-IoT. In Proc. ICCMC (pp. 354–357). IEEE.

[10] Ho¨jer, M., & Wangel, J. (2015). Smart sustainable cities: Definition and challenges. In ICT Innovations for Sustainability (pp. 333–349). Springer.

[11] Russell, C. (2018). SDG 11: Sustainable Cities and Communities. BGjournal, 15, 31–33.

[12] Janzen, Y., Luna, A., & Ramaj, V. (2015). Real-time access control based on facial recognition. In Proc. ICCMC.

[13] Carrick, M., & Ozen, F. (2012). A Face Recognition System Based on Eigenfaces Method. IJCA, 60(2), 23–28.

[14] Carli, R., Cavone, G., Othman, S. B., & Dotoli, M. (2020). IoT-based architecture for model predictive control of HVAC systems in smart buildings. Sensors, 20(3), 781.

[15] Ghayvat, H., Mukhopadhyay, S., Gui, X., & Suryadevara, N. (2015). WSN- and IoT-based smart homes and their extension to smart buildings. Sensors, 15(5), 10350–10379.

[16] Moudoud, H., Khoukhi, L., & Cherkaoui, S. (2022). Prediction and detection of FDIA and DDoS attacks in 5G-enabled IoT. arXiv preprint.

[17] Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for IoT: Communication technologies and challenges. IEEE Access, 6, 3619–3647.

[18] Yang, C., Liang, P., Fu, L., Cui, G., Huang, F., Teng, F., & Bangash, Y. A. (2022). Using 5G in smart cities: A systematic mapping study. Information Systems and Applications.

[19] Bartelt, J. (2023). Sustainable Smart Cities: The Role of Telecoms in Shaping the Future. STL Partners.

[20] Meng, Z., Wu, Z., & Gray, J. (2017). A collaboration-oriented M2M messaging mechanism for future industrial networks. Sensors, 17(11), 2694.

[21] Chandeliya, N., Chari, P., Karpe, S., & Karia, D. C. (2020). Reliable M2M communication using MQTT protocol and MEAN stack. In ICIDCA (pp. 109–120). Springer.

[22] Rong, B., Han, S., Kadoch, M., Chen, X., & Jara, A. (2020). Integration of 5G networks and IoT for future smart city. Wireless Communications and Mobile Computing.

[23] Chauhan, S., & Popat, K. (2023). Optimizing business models through IoT-enabled M2M protocols. IJISAE.

[24] Ruby, K. E. D., Pushpavalli, M., Selvarani, A., Thilagavathy, S. D., Choubey, S. B., & Harika, D. (2024). Smart device-M2M approach for enhancing communication in MANET using IoT and cloud. IJISAE.

[25] Han, H., Zhai, W., & Zhao, J. (2021). Smart city enabled by 5G/6G networks: An intelligent hybrid random access scheme. arXiv preprint.

[26] Namdar, J. H., & Yonan, J. F. (2023). Revolutionizing IoT security in the 5G era with AI-powered solutions. Babylonian Journal of IoT.

[27] Alliheedi, M., et al. (2023). 5G networks and IoT devices: Mitigating DDoS attacks with deep learning. arXiv preprint.

[28] Author(s) (2024). 5G-enabled smart cities: Evaluation of pilot applica- tions. Internet of Things Journal.

[29] Author(s) (2024). A survey on 5G and LPWAN-IoT for improved smart cities and remote applications. Sensors.

[30] Author(s) (2024). A comprehensive study on IoT privacy and security challenges with focus on 5G/6G. High-Confidence Computing.

[31] Banerjee, A., & Sharma, S. (2024). 5G-enabled smart cities: A real- world evaluation and analysis. *ScienceDirect*.

[32] Rachakonda, L. P. (2024). A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *ScienceDirect*.

[33] Mahomed, A. S. (2025). Unleashing the potential of 5G for smart cities: A focus on real-time digital twins. *MDPI*.

[34] Kapoor, A. (2024). Transforming smart cities: Intersection of 5G tech- nology and IoT. *SSRN*.

[35] Sharma, S. (2024). Data-driven smart cities: Integrating the power of 5G and IoT. *PES Journal*.