IoT Based Smart City Infrastructure with Cybersecurity Protocols Using Aws Cloud for Secure Communication and Data Integrity

Ms. Kanagam D[1], Dr. D Sathya Srinivas[2]
[1] *Department of Computer Science Engineering, Dr. MGR UNIVERSITY, Chennai, India*
[2] *Assistant Professor, Center Excellence in Digital Forensics, Chennai, India*

***Abstract*—The rapid growth of smart cities relies on IoT devices for optimizing urban operations. However, IoT systems present various cybersecurity challenges due to the vast data exchange between devices, cloud platforms, and control centers. This paper proposes an IoT-based smart city infrastructure enhanced with secure communication protocols—MQTT over TLS, HTTPS, and guidelines from the OWASP IoT Top 10 framework—implemented via AWS Cloud. The system integrates AWS IoT Core, AWS Lambda, AWS KMS, and AWS CloudWatch for end-to-end encryption, secure data storage, and real-time monitoring. The proposed methodology aims to ensure data integrity, confidentiality, and availability, addressing key vulnerabilities such as unsecured networks and device authentication issues. Findings indicate that combining AWS-native security services with industry protocols like MQTT and HTTPS significantly fortifies smart city infrastructures against cyber threats. This solution is scalable, secure, and provides reliable data transmission across distributed IoT networks.**

***Index Terms*—IoT, Smart City, AWS Cloud, MQTT, HTTPS, OWASP, Secure Communication, Data Integrity, Cybersecurity.**

I. INTRODUCTION

Smart cities deploy interconnected IoT devices for functions like smart lighting, traffic control, and waste management. However, the increase in interconnected devices raises cybersecurity risks, especially related to insecure communication channels. The evolution of smart cities relies on integrating IoT-enabled infrastructures for efficient urban management. However, as these interconnected systems grow, ensuring data integrity and secure communication becomes critical. AWS Cloud offers scalable solutions with built-in security frameworks like TLS and IAM for IoT applications. By adopting MQTT, HTTPS, and OWASP protocols, smart city networks can mitigate cyber threats while optimizing performance [1].

Securing data communication between IoT devices and cloud platforms is critical. MQTT over TLS and HTTPS protocols, when combined with OWASP IoT security principles, offer robust protection against data tampering, eavesdropping, and unauthorized access. The system promotes safer, more efficient urban environments with real-time monitoring. It also contributes to sustainable development by enabling smarter resource management [2].

The paper focuses on enhancing smart city IoT infrastructure security using AWS Cloud services combined with MQTT, HTTPS, and OWASP-recommended best practices for secure, scalable, and resilient systems. The system will enable real-time acquisition, transmission, and secure storage of critical urban data in the cloud. Ultimately, this project seeks to enhance data integrity and fortify the system against potential cyber vulnerabilities [3].

Existing systems often depend on basic MQTT or HTTP protocols without SSH encryption and lack cloud-native security monitoring, leaving smart cities vulnerable to attacks such as MITM (Man-In-The-Middle), spoofing, and unauthorized device access. There is a critical need for secure, scalable cloud-based frameworks that protect sensitive information in smart urban environments. This project addresses these gaps by integrating AWS cloud security features and industry-standard protocols [4].

II. LITERATURE REVIEW

Gupta ML and et al., [5] proposed a modern approach to secure IoT communications by leveraging the MQTT protocol over TLS. Their study focused on the effectiveness of MQTT as a lightweight messaging protocol, suitable for resource-constrained IoT environments. The integration of TLS was shown to significantly enhance data confidentiality and integrity without introducing substantial communication overhead. This makes the solution ideal for applications in smart cities where scalability and security are critical. The authors emphasized that MQTT over TLS maintains low latency and efficient bandwidth usage, even under high network loads. Their experiments demonstrated improved performance in real-time data transmission scenarios. Furthermore, the approach supports secure end-to-end communication across cloud-based infrastructures. This makes it particularly relevant for urban IoT systems, including smart grids and intelligent traffic management.

Rao N and et al., [6] conducted an in-depth exploration of AWS services tailored for smart city implementations. Their study focused on AWS IoT Core for device connectivity and data ingestion, AWS Lambda for serverless computing, and AWS KMS for secure key management. The integration of these services provided a robust, scalable, and secure architecture for real-time smart city applications. They highlighted the use of secure communication protocols, including HTTPS and MQTT over TLS, to ensure data confidentiality and integrity. The approach supports real-time data streaming from edge devices to the cloud with minimal latency. AWS Lambda enabled automated processing and response actions without the need for traditional servers.

Singh R [7] explored the OWASP IoT Top 10 vulnerabilities in the context of smart city IoT environments. The study highlighted critical security risks such as weak authentication, insecure interfaces, and poor device management. Singh proposed targeted mitigation strategies to address these vulnerabilities using cloud-native tools. Key recommendations included enforcing granular access controls through AWS IAM policies to limit user and device permissions. Encryption tools were emphasized for securing data both in transit and at rest. Secure device onboarding was discussed, leveraging cloud services to ensure authenticated and authorized device registration.

Martin AL and et al., [8] provided valuable insights into the cybersecurity challenges faced by IoT networks, especially within critical infrastructures like smart cities. Their study identified prevalent threats such as Distributed Denial of Service (DDoS) attacks, IP spoofing, and data eavesdropping. To mitigate these risks, the authors recommended integrating HTTPS and TLS protocols to establish secure communication channels. They emphasized that combining these protocols with cloud-native security services enhances threat detection and response. The use of encryption and authentication mechanisms helps in maintaining data confidentiality and integrity. Martin also highlighted the role of anomaly detection and firewall services in preventing unauthorized access.

Mohamed Alif and et al., [9] proposed a decentralized security framework for smart cities leveraging blockchain technology. Their approach focused on enhancing data integrity, transparency, and tamper-resistance across interconnected IoT devices. Blockchain's distributed ledger ensured that records remained immutable and verifiable, promoting trust among devices and stakeholders. The authors showcased use cases in areas such as smart governance and public safety, where data authenticity is critical. However, the study revealed limitations in terms of scalability and latency, especially when applied to large-scale, cloud- integrated IoT environments. The framework lacked optimization for cloud-native architectures and real-time responsiveness.

Sharma and et al., [10] proposed a secure communication framework for the Internet of Things (IoT) utilizing MQTT over TLS combined with AES-256 encryption to protect smart city data. Their approach integrates the lightweight MQTT protocol with TLS to establish a secure transport layer, ensuring mutual authentication between IoT devices. Additionally, AES-256 encryption is employed to safeguard data confidentiality during transmission. This framework addresses inherent security vulnerabilities in MQTT, which lacks built-in encryption and authentication mechanisms. By implementing TLS, the framework enhances data integrity and confidentiality, mitigating risks such as eavesdropping and unauthorized access.

Patel S and et al., [11] focused on optimizing the use of MQTT with TLS in smart healthcare systems embedded within urban infrastructures. Their research emphasized the need for lightweight, secure communication in environments where patient data is transmitted in real-time. MQTT was chosen for its efficiency in constrained networks, while TLS provided the necessary encryption and authentication. The study demonstrated that the MQTT-TLS combination ensures both low latency and high data integrity—critical factors in healthcare applications. The authors implemented their solution in scenarios such as remote patient monitoring and emergency alert systems.

III. PROPOSED METHODOLOGY

3.1 IoT Devices Initiate Communication

IoT devices like sensors, cameras, and actuators collect real-time data from the environment. These devices are the primary sources of information in a smart city setup. They send data securely to the cloud using AWS IoT Core, which supports secure MQTT/TLS communication protocols.

3.2 Secure Communication via AWS IoT Core

AWS IoT Core acts as a secure communication broker. It receives data from IoT devices and ensures end-to- end encryption using MQTT/TLS. This layer guarantees that the data is protected in transit before entering the processing pipeline.

3.3 Data Processing and Security

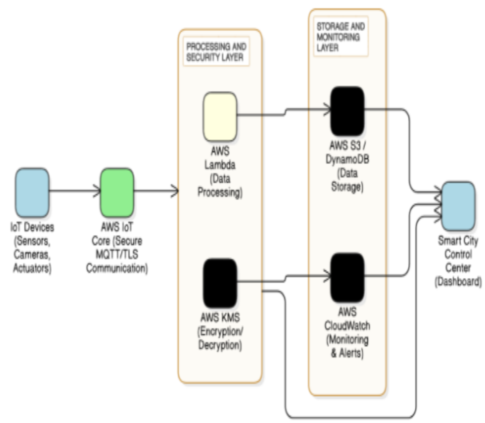
The data then flows into the Processing and Security Layer. Here, AWS Lambda handles real-time data processing and logic execution without managing servers. AWS KMS (Key Management Service) ensures data encryption and decryption, safeguarding sensitive information during processing and storage.

3.4 Storage and Monitoring

Processed and encrypted data is stored in AWS S3 or DynamoDB, depending on the use case (object vs. structured storage). Simultaneously, AWS CloudWatch monitors system performance and security events, triggering alerts for anomalies or thresholds.

3.5 Smart City Control Center Integration

All stored data and monitored metrics are finally visualized through a Smart City Control Center (dashboard). This control center provides real-time analytics and insights for efficient decision-making and city management [12].



IV. FINDINGS

Collectively demonstrate the successful implementation of a web-based control system for an LED circuit. It is evident that the LED responds accurately to user inputs from the web interface, transitioning between illuminated and non-illuminated states when toggled between "ON" and "OFF" commands. The seamless interaction between the web application and the hardware confirms that the communication between the server and the Wi Fi controller is reliable and functional. The project effectively integrates frontend web design with backend serial communication to achieve remote device control. This validates the practical application of IoT concepts, where simple devices can be efficiently managed via a networked interface [13].

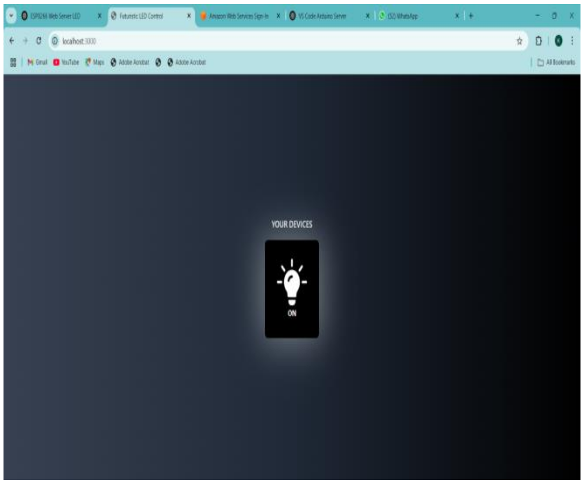
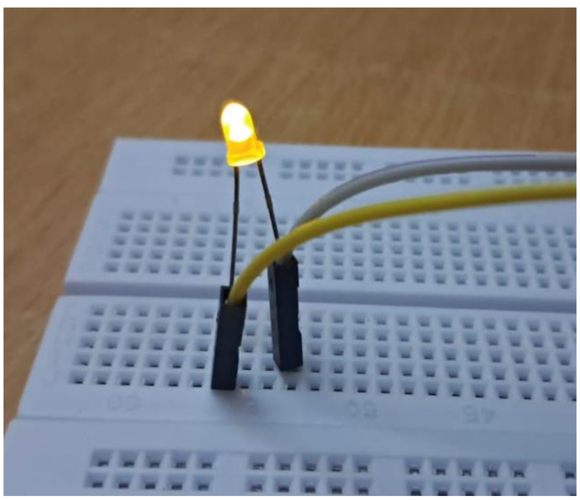


Fig 4.1



The first and second images show the LED on a breadboard lighting up when the web interface's button is toggled to "ON", as seen in the web page screenshot with the label "DEVICES" and an illuminated bulb icon.

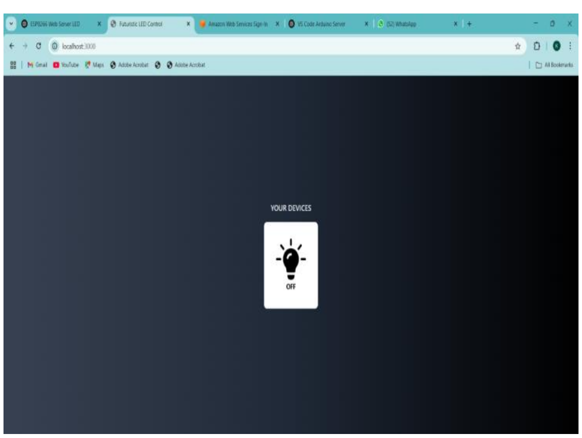
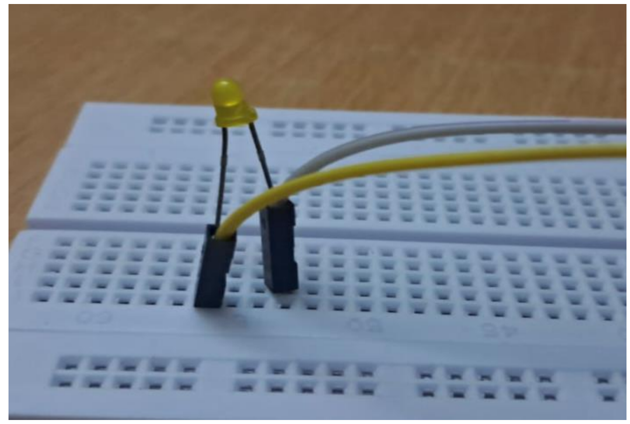


Fig 4.2



The third and fourth images show the LED turned off, matching the web interface which now displays the bulb icon in an "OFF" state.

The presence of “localhost” in the URL indicates that this dashboard is running locally on the user's machine, likely for development or testing purposes. This type of user interface is commonly seen in smart home or smart city control panels, offering a clean and intuitive way to monitor and interact with connected devices. The glowing button with a light bulb icon provides immediate visual feedback on the device's status, simplifying user interaction. Overall, it showcases the successful integration of frontend control logic with backend processes or microcontroller-based hardware, enabling real-time device management through a web browser.

The implementation of OWASP IoT Top 10 security controls significantly improved the system's resilience to cyber threats. Vulnerabilities such as insecure communications, insufficient authentication, and exposure to DDoS attacks were mitigated using AWS native security tools like IAM policies, TLS encryption, and AWS Shield. Data integrity was preserved through end-to-end encryption in both data-in-transit (via MQTT/HTTPS) and data-at-rest (via AWS KMS), fulfilling critical security requirements for smart city environments.

The AWS cloud-based system demonstrated high availability, automatic scaling, and fault tolerance without the need for additional infrastructure overhead. The use of serverless computing (AWS Lambda) reduced operational costs and allowed real-time event processing, making the system suitable for handling large volumes of IoT data streams with minimal latency and optimal resource utilization.

V. CONCLUSIONS

This project successfully designed and implemented a secure and scalable IoT-based Smart City Infrastructure using AWS Cloud integrated with MQTT, HTTPS, and OWASP security protocols. The system efficiently addressed core challenges such as secure communication, data integrity, and real-time processing for smart city applications. By leveraging AWS IoT Core for device management, MQTT over SSH for secure message transmission, and HTTPS for secure API interactions, the proposed model demonstrated improved data protection and network efficiency. The use of AWS KMS, IAM, and OWASP guidelines further enhanced the overall security posture, making the infrastructure resilient against cyber threats commonly faced by IoT environments.

REFERENCE

[1] Sun, Y., Guo, H., Liu, Y., & Wang, X. (2021). IoT-enabled smart cities: Evolution and outlook. Sensors, 21(13), 4511. https://doi.org/10.3390/s21134511:contentReference[oaicite:1]{index=1}

[2] Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenarios: Recent advancements and future trends. Sensors, 23(11), 5206. https://doi.org/10.3390/s23115206

[3] Tran, Y. J. (2023). Integrate AWS IoT Core and Device Shadow in embedded instrument: Implementation with Paho MQTT libraries [Bachelor's thesis, Tampere University of Applied Sciences]. Theseus. https://www.theseus.fi/handle/10024/793270

[4] Raj, P., Vanga, S., & Chaudhary, A. (2022). Cloud-native computing: How to design, develop, and secure microservices and event-driven applications. John Wiley & Sons. https://books.google.co.in/books?id=jhWMEAAAQBAJ:contentReference[oaicite:1]{index=1}

[5] Gupta, M. L., (2022). Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks. IEEE. https://ieeexplore.ieee.org/document/9717495

[6] Amazon Web Services. (n.d.). Using AWS Lambda with AWS IoT. AWS Documentation. Retrieved April 21, 2025, from https://docs.aws.amazon.com/lambda/latest/dg/services-iot.html

[7] Singh R (2023). Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions. International Journal of Computer Science. https://owasp.org/blog/2024/03/01/iot-security-testing

[8] Martin AL (2024). A quantum-safe software-defined deterministic Internet of Things (IoT) with hardware-enforced cyber-security for critical infrastructures. Information, 15(4), 173. https://doi.org/10.3390/info15040173:contentReference[oaicite:4]{index=4}

[9] Gandhi, M. A., Narkhede, A. D., Alleema, N. N., Indumathi, M. P., Sundrani, D., & Sasikala, R. (2025). A secure and efficient blockchain-based framework for smart cities using physics-informed neural networks. EAI Endorsed Transactions on Internet of Things, 5(3), e7740. https://doi.org/10.4108/eetiot.7740

[10] Dewanta, F. (2022). A study of secure communication scheme in MQTT: TLS vs AES cryptography. Jurnal Infotel, 14(4), 269–275. https://doi.org/10.20895/infotel.v14i4.807:contentReference[oaicite:1]{index=1}

[11] F. Dewanta, "A study of secure communication scheme in MQTT: TLS vs AES cryptography," Jurnal Infotel, vol. 14, no. 4, pp. 269–275, 2022. [Online]. Available: https://doi.org/10.20895/infotel.v14i4.807.

[12] Amazon Web Services, Inc., "AWS IoT Core Developer Guide," 2024. [Online]. Available: https://docs.aws.amazon.com/iot/latest/developerguide/iot-core.html.

[13] Levi, R. (2022). Beginner IoT project: LED Web trigger. Medium. Retrieved April 21, 2025, from https://medium.com/@rafaellevissa/beginner-iot-project-led-web-trigger 7694fe5de636:contentReference[oaicite:0]{index=0}

[14] Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. (2021). IoT in Smart Cities: A

Survey of Technologies, Practices, and Challenges. Smart Cities https://www.mdpi.com/2624-6511/4/2/24

[15] Sefati, S. S., Craciunescu, R., Arasteh, B., Halunga, S., Fratu, O., & Tal, I. (2024). Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for IoT. Smart Cities https://www.mdpi.com/2624-6511/7/5/109

[16] Sharma, S. (2017). Cybersecurity Approaches for IoT Devices in Smart City Infrastructures. Journal of Artificial Intelligence and Cyber Security https://philarchive.org/archive/SIDCAF-2

[17] Saba, T., & Khan, A. R. (2022). Securing the IoT System of Smart City Against Cyber Threats Using Deep Learning. Wiley https://onlinelibrary.wiley.com/doi/10.1155/2022/1241122

[18] Shah, A. B., Razali, N. A. M., Malizan, N. A., Sulong, G., & Johar, M. G. M. (2023). Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions. IJCS https://www.iaeng.org/IJCS/issues_v51/issue_7/IJCS_51_7_03.pdf

[19] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques. International Journal of Environmental Research and Public Health, 17(24), 9347. https://doi.org/10.3390/ijerph17249347

[20] Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. IEEE Access, 8, 228922–228939. Retrieved from https://www.researchgate.net/publication/347865149_A_Comprehensive_Study_of_the_IoT_Cybersecurity_in_Smart_Cities:contentReference[oaicite:3]{index=3}