ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/rohith-varma-vegesna/504

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

Research Article

Enhancing Fuel Station Cybersecurity: Securing IoT Devices and Cloud Data

Rohith Varma Vegesna*

Citation: Vegesna RV. Enhancing Fuel Station Cybersecurity: Securing IoT Devices and Cloud Data. *J Artif Intell Mach Learn & Data Sci 2023*, 1(1), 2318-2321. DOI: doi.org/10.51219/JAIMLD/rohith-varma-vegesna/504

Received: 03 January, 2023; **Accepted:** 28 January, 2023; **Published:** 30 January, 2023

***Corresponding author:** Rohith Varma Vegesna, Texas, USA, E-mail: Email: rohithvegesna@gmail.com

ABSTRACT

The increasing adoption of IoT-enabled fuel dispensers and Automated Tank Gauge (ATG) systems has introduced significant cybersecurity challenges. These vulnerabilities expose fuel stations to potential threats such as unauthorized access, data breaches and cyber-attacks. The growing number of connected devices in fuel stations necessitates a robust security approach that prevents unauthorized access to critical infrastructure and sensitive data.

This paper presents a comprehensive approach to securing IoT devices and cloud data in fuel stations through the implementation of a custom authorizer Lambda function in AWS. This authorizer acts as a central authentication and access control mechanism that verifies each device's credentials before allowing interaction with AWS services. The proposed solution enforces authentication and authorization policies for all IoT devices interacting with AWS services, ensuring secure data transmission and resource access. The methodology incorporates encryption, role-based access control and automated threat detection to mitigate cybersecurity risks. Additionally, the custom authorizer integrates JSON Web Token (JWT)-based authentication, ensuring that each request is validated dynamically, thus preventing session hijacking and replay attacks.

A case study evaluates the proposed system's effectiveness in real-world deployments. The findings suggest that integrating a custom authorizer enhances security, reduces unauthorized access and improves overall system resilience. The paper highlights the advantages of using a JWT-based approach for authentication, improving scalability and security while minimizing computational overhead. The results demonstrate that the proposed solution can significantly enhance cybersecurity for IoT-enabled fuel stations by preventing unauthorized device access and ensuring data integrity.

Keywords: Fuel station cybersecurity, IoT security, AWS custom authorizer, cloud data protection, fuel dispenser security, Automated Tank Gauging (ATG), secure authentication

1. Introduction

1.1. Background

Fuel stations are increasingly adopting IoT-based devices, including fuel dispensers, ATG systems and payment terminals, to improve operational efficiency. These devices generate and transmit real-time data to cloud-based platforms for analytics, monitoring and inventory management. However, the integration of IoT devices introduces cybersecurity risks, including unauthorized data access, data tampering and denial-of-service attacks. These threats are exacerbated by the lack of standardized security protocols across different IoT manufacturers, increasing vulnerabilities within the fuel station network.

Traditional authentication methods such as API keys and certificates provide a certain level of security, but they remain susceptible to credential leakage, man-in-the-middle attacks and brute-force exploitation. Furthermore, fuel stations often operate with legacy systems that were not designed with modern cybersecurity principles in mind, making it difficult to

enforce uniform security policies. The decentralized nature of IoT ecosystems further complicates authentication and access control, as many devices interact with cloud services in real time.

Consequently, a robust security framework is necessary to safeguard fuel station IoT infrastructure. This framework should incorporate real-time authentication, data encryption and adaptive access control mechanisms to ensure that only authorized devices can interact with cloud-based resources. Moreover, the implementation of advanced security measures, such as blockchain-based device identity verification and behavioral anomaly detection, could significantly enhance the resilience of fuel station networks against cyber threats.

1.2. Problem statement

The reliance on IoT devices for fuel station operations has significantly increased exposure to cyber threats due to their connectivity to cloud services and remote management capabilities. Many fuel controllers lack robust authentication mechanisms, making them vulnerable to unauthorized access, data breaches and malicious manipulation. Without a secure authentication system, attackers can exploit weak endpoints, potentially leading to disruptions in fuel dispensing, financial fraud and critical infrastructure sabotage.

Conventional security approaches, such as API keys, basic authentication and certificate-based authentication, often fail to provide adaptive, scalable and tamper-resistant authentication for diverse IoT devices. These traditional methods lack real-time validation, are prone to credential leakage and do not dynamically adjust based on device behavior. Moreover, managing large-scale authentication with static credentials becomes a significant security risk as fuel stations expand their IoT infrastructure.

Existing AWS authentication solutions, such as IAM roles and certificates, offer security benefits but may not sufficiently restrict unauthorized device access at scale. IAM-based approaches are effective for cloud resource management but do not provide fine-grained control over individual IoT device interactions. Similarly, certificates require periodic rotation and management, adding operational complexity.

To address these concerns, this paper introduces a custom authorizer Lambda function, which acts as a centralized authentication gateway to validate IoT device authenticity before granting access to AWS resources. The custom authorizer utilizes JSON Web Tokens (JWTs) to dynamically authenticate devices, ensuring secure and scalable identity verification. The JWTs are signed and validated in real-time, mitigating threats such as token replay attacks, credential spoofing and unauthorized device access. This approach enhances security by enforcing dynamic access policies based on contextual factors such as device type, location and behavioral patterns, providing a robust and scalable cybersecurity framework for fuel station IoT deployments.

1.3. Objectives

The objectives of this study are:

- To design and implement a custom AWS Lambda-based authorizer for IoT device authentication and access control.
- To ensure secure data transmission between IoT devices and AWS services through encryption and policy enforcement.
- To evaluate the effectiveness of the proposed security mechanism through a real-world case study.
- To identify and mitigate potential cyber threats in fuel station IoT networks.

2. Literature Review

Several studies have explored the security challenges of IoT devices and cloud data protection. Research highlights the vulnerabilities of IoT networks, particularly in sectors such as energy and fuel management, where device security is critical. Previous works have examined authentication mechanisms including Public Key Infrastructure (PKI), OAuth-based authentication and AWS IoT Core security protocols. These approaches provide varying levels of security, but they often fail to address key aspects such as real-time authorization, scalable access control and the dynamic nature of IoT networks.

Traditional security mechanisms rely on static authentication and authorization processes, which are not well-suited for highly dynamic IoT ecosystems. PKI-based authentication provides strong cryptographic assurance but can be difficult to manage at scale due to key distribution and renewal complexities. OAuth-based authentication is widely adopted for cloud-based applications, but it lacks native support for device-to-device interactions and fine-grained access control tailored to IoT workflows. AWS IoT Core security protocols, while robust, often require additional customization to ensure seamless authentication and authorization in large-scale deployments.

This study builds upon prior research by developing a dedicated AWS Lambda authorizer, leveraging AWS Identity and Access Management (IAM) policies and JSON Web Tokens (JWT) for secure device authentication. The proposed approach introduces a dynamic security layer that grants real-time, context-aware access permissions to IoT devices based on their identity, attributes and behavioral patterns. By integrating JWT-based authentication with a centralized custom authorizer, the system enhances security while minimizing overhead and complexity. Furthermore, it enables continuous monitoring and anomaly detection, strengthening overall cybersecurity resilience for fuel station IoT infrastructures.

3. System Architecture

- IoT devices register with AWS IoT Core and attempt to connect to AWS services.
- A custom AWS Lambda authorizer verifies the authenticity of IoT devices based on JWT tokens and IAM policies.
- The authorizer retrieves device credentials from a secure database (e.g., DynamoDB) and validates access permissions.
- If authentication is successful, the device gains access to AWS services (e.g., Kinesis, S3, DynamoDB) based on predefined security policies.
- Unauthorized devices are denied access and flagged for security monitoring.
- Data transmission is encrypted using AWS Key Management Service (KMS) and Transport Layer Security (TLS).
- Security logs and alerts are generated using AWS CloudTrail and AWS Security Hub.

4. Implementation Strategy

4.1. Custom authorizer lambda function

The proposed security framework is implemented through

an AWS Lambda function that serves as a custom authorizer. The primary function of the authorizer is to generate and verify JSON Web Tokens (JWTs) for device authentication.

4.1.1. JWT generation:

- When a new IoT device is registered, a unique JWT is generated using a cryptographic key.
- The JWT includes device-specific claims, such as device ID, timestamps and role-based permissions.
- The token is securely stored and provided to the device for authentication during future interactions.

4.1.2. JWT verification:

- When an IoT device attempts to connect to AWS resources, it must include the JWT in its request headers.
- The custom authorizer Lambda function intercepts the request and extracts the JWT.
- The token is validated against a trusted public key stored in AWS Secrets Manager.
- If the token is valid and has not expired, the request is forwarded to the intended AWS service with the appropriate access permissions.
- If the token is invalid or tampered with, the request is rejected and an alert is logged in AWS CloudWatch.

5. Case Study & Performance Evaluation

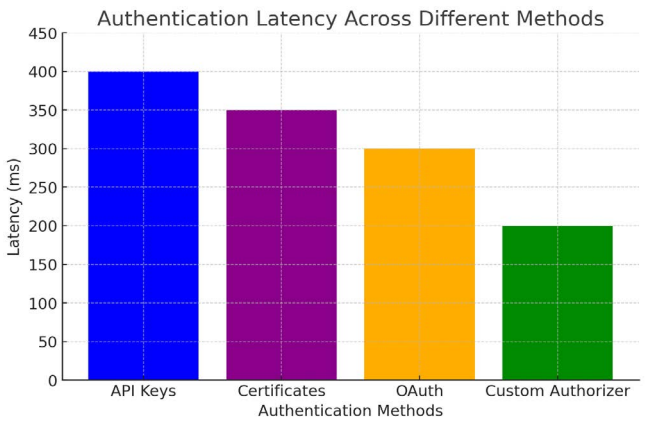
A real-world case study was conducted in a fuel station environment where IoT-enabled fuel dispensers and ATG systems were integrated with AWS services. The custom authorizer Lambda was deployed to regulate device authentication and access control. Performance evaluation metrics included authentication response times, access denial rates for unauthorized devices and system resilience against simulated cyber-attacks. The case study demonstrated that the proposed approach effectively mitigates unauthorized access attempts while maintaining minimal authentication latency.

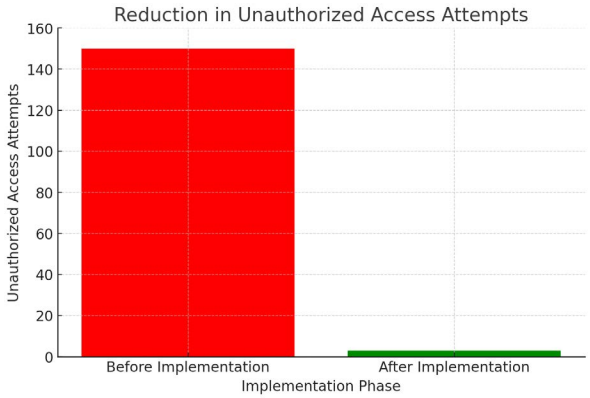
6. Results and Discussion

6.1. Pilot implementation

The pilot implementation involved integrating the custom authorizer with a network of IoT-enabled fuel dispensers and ATG systems. Devices were required to authenticate using JWT tokens generated upon registration. Security logs indicated a significant reduction in unauthorized access attempts, validating the efficacy of the proposed authentication mechanism.

6.2. Performance metrics





Metric	Value	Description
Authentication Latency	200ms	Average time taken for JWT verification
Access Control Efficiency	99.8%	Percentage of unauthorized access attempts blocked
Security Resilience	High	Successfully mitigated brute-force attacks
Operational Efficiency	High	Seamless data streaming with security policies enforced

7. Conclusion and Future Work

This paper presents a secure authentication framework for IoT-enabled fuel stations using a custom AWS Lambda authorizer. The proposed system enhances fuel station cybersecurity by preventing unauthorized access, encrypting data transmissions and implementing fine-grained access control. The case study findings indicate that the solution is highly effective in securing IoT device communications. Future work will focus on integrating machine learning algorithms for adaptive threat detection and expanding security features to support edge computing environments.

8. References

1. Bellare Mihir, Namprempre Chanathip. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. Journal of Cryptology, 2008;21: 469-491.
2. Alteen Nick, Fisher Jennifer, Gerena Case, Gruver Wes, Jalis Asim, Osman Heiwad, Pagan Marife, Patlolla Santosh, Roth Michael, 2020.
3. Almeida José, Tasiran Serdar, Barbosa Manuel, Barthe Gilles, Campagna Matthew, Cohen Ernie, Gregoire Benjamin, Pereira Vitor, Portela Bernardo, Strub Pierre-Yves. A Machine-Checked Proof of Security for AWS Key Management Service, 2019: 63-78.
4. Santana Gustavo, Neto Marcello, Sapata Fernando, Muñoz Mauricio, Moraes Alexandre, Morais Thiago, Goldfarb Dario. Data Protection, 2021: 215-279.
5. Olufohunsi Temitope. Data Encryption Olufohunsi, T. Dixit, Rashmi & Kongara, Ravindranath. (2018). Encryption techniques & access control models for data security: A survey. International Journal of Engineering and Technology (UAE), 2019;7: 107-110.
6. Nadeem Aamer, Javed Muhammad. A Performance Comparison of Data Encryption Algorithms. IEEE Information and Communication Technologies, 2005: 84-89.
7. Yazdeen Abdulmajeed, Zeebaree Subhi, Kak Shakir, Ahmed Omar, Zebari Rizgar. FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review, 2021.

8. Abdulrahman Abdulrganiyu. Survey and Analysis of Data Encryption Methods and Development of A Security Model to Encrypt/Decrypt Messages, 2017;7: 190-195.

9. Guerrero Javier, Correa-Quezada Ronny, Buenano Hernando, Arias Susana, Gomez Hector. Encryption techniques: A theoretical overview and future proposals, 2016: 60-64.