Integrating Spatio-temporal Authorization With Generic Cloud-based Software Architecture for Internet Of Things Devices

Marshal Moncivais*,Mustafa Al Lail
School of Engineering, Texas A&M International University, Laredo, Texas, 78041

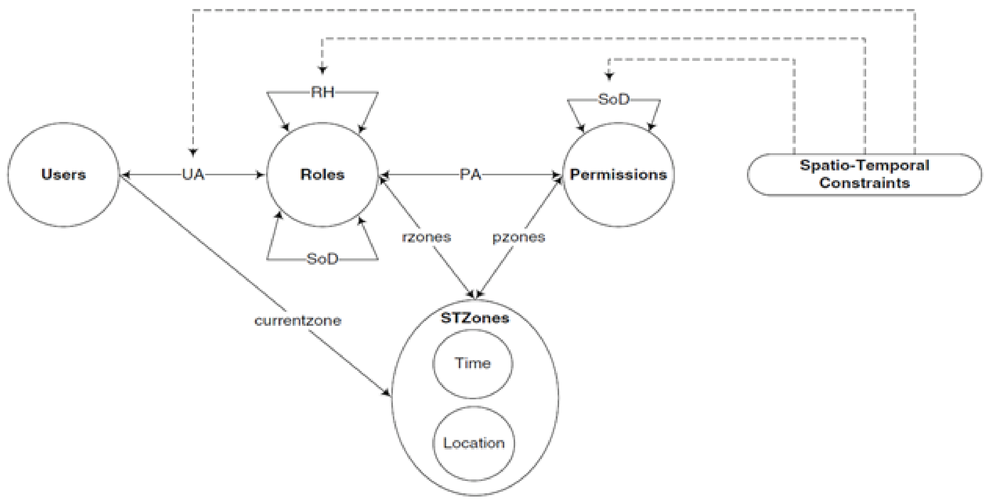
Introduction

Recently, there has been a significant rise in the use of Internet-of-Things (IoT) in various areas of society. Because these systems tend to have weaker security, they pose a larger risk when integrated into cloud systems. This problem is compounded by a lack of a standardized IoT model, meaning that diagnosing security issues for IoT systems as a whole is more difficult. If IoT systems could adhere to a standard architecture that incorporates spatio-temporal access control, they could be made more secure overall.

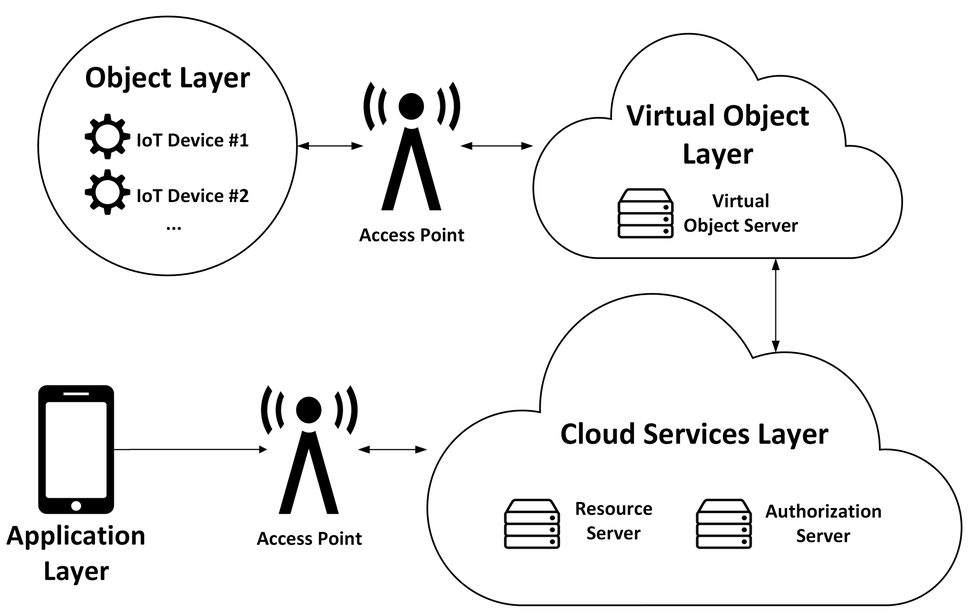
Problem and Objective

- **Problem:**
  - Current IoT systems lack a standardized model and lack consistent support for determining access control decisions based on spatio-temporal constraints.
- **Objectives:**
  - Design a 4-layered software architecture based on the proposed model by Alsheri and Sandhu [3] that incorporates spatio-temporal access control.
  - Apply a secure communications protocol to safeguard messages.
  - Create a software implementation that demonstrates the process of accessing IoT devices within this software architecture.

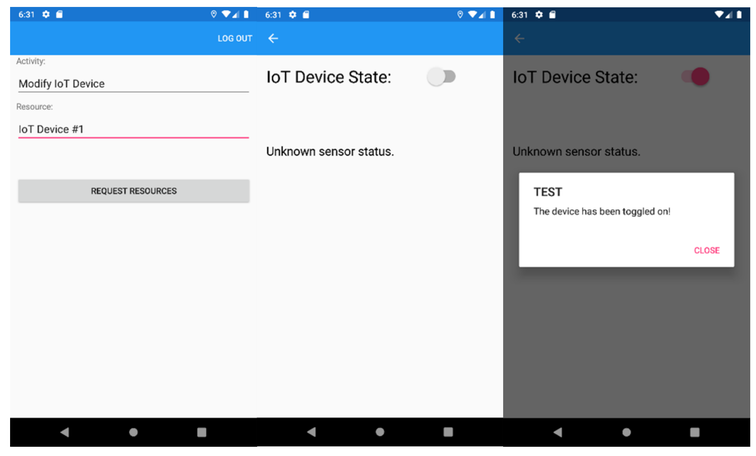
Conceptual GSTRBAC Model



IoT Software Architecture



IoT Mobile Application



Software Architecture Layers

Application Layer – Contains applications in the system that can interact with IoT devices and data stored from IoT devices.

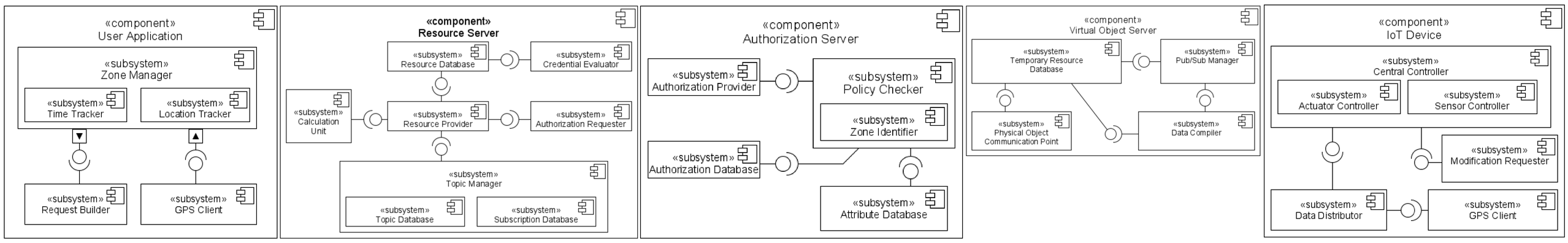
Cloud Services (CS) Layer – Contains servers that manage data storage of data and authorization for access requests in the system. There are two types of servers in this layer:

- The **Resource Server** stores IoT device information long-term and distributes that information to the application layer when requested.
- The **Authorization Server** makes access control decisions on whether IoT devices or their information should be accessed or not based on a user's role and the time and location of access.

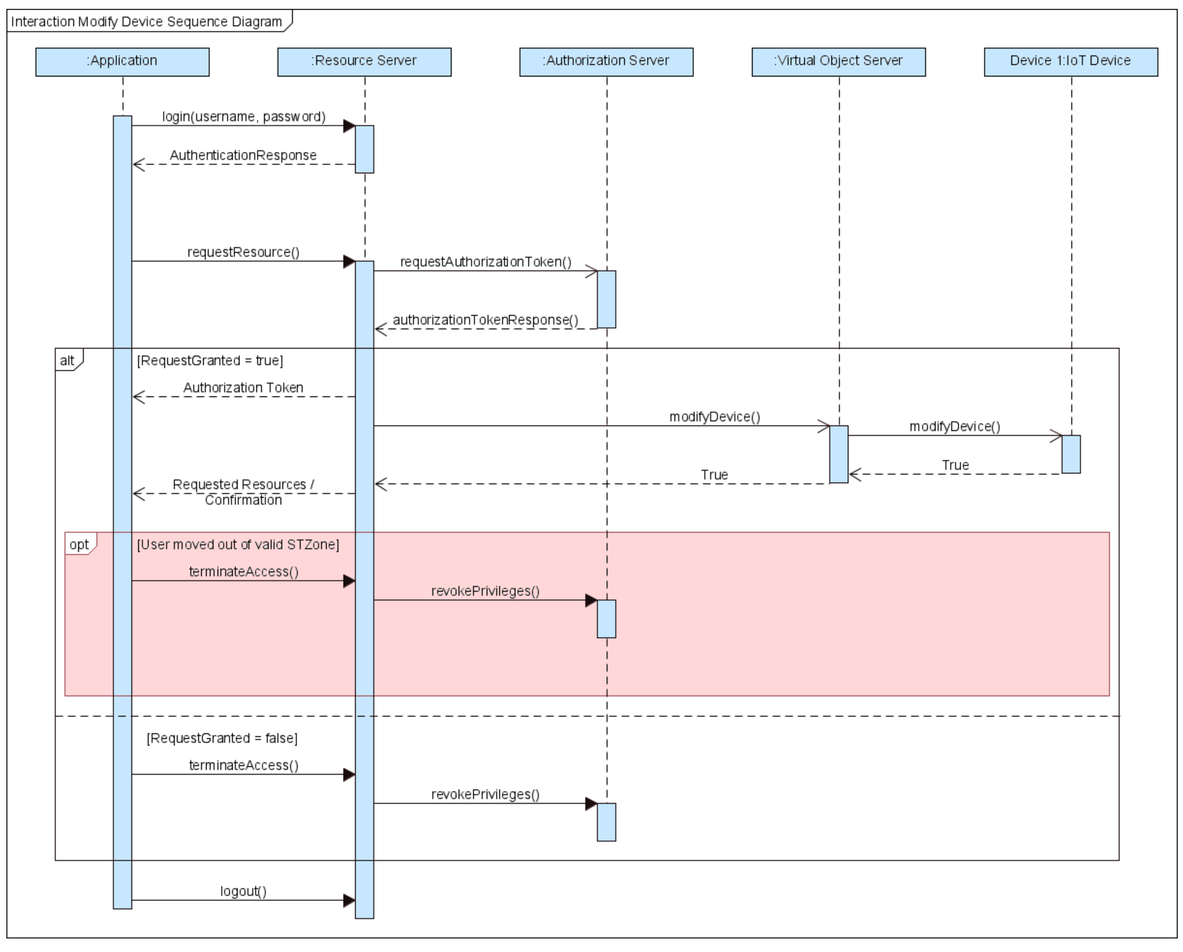
Virtual Object (VO) Layer – Contains servers that act as an abstraction of IoT devices. These servers contain information about the past state, current state, and estimated future state of connected IoT devices.

Object Layer – Contains physical IoT devices in the system. These devices have a limited capacity to store data and perform actions in the real world.

Software Architecture Components



Secure Communication Protocol Sequence Diagram



Secure Communication Protocol

Two security protocols are employed in this system:

Lightweight protocol – This symmetric protocol uses multiple cryptographic algorithms to secure communications between components.

- The handshake protocol that exchanges key information uses Elliptic Curve Diffie-Hellman (ECDH).
- The encryption/decryption protocol uses Advanced Encryption Standard (AES).
- The digital signature protocol used for message authentication uses Elliptic Curve Digital Signature Algorithm (ECDSA).

This protocol is only used in the communication between the VO Layer and the Object Layer because it is less computationally intensive.

Heavyweight protocol – This asymmetric protocol uses a single computationally intensive cryptographic algorithm to secure communications between components.

- The handshake protocol, message encryption/decryption, and digital signature functions all use RSA.

This protocol is used for communication between the Application Layer, CS Layer, and VO Layer.

Conclusion

- Designed a generic 4-layer software architecture for cloud-based IoT systems that incorporates spatio-temporal constraints into access control decisions.
- Created a simple application that demonstrates the communication protocol for this software architecture.

References

[1] R. Abdunabi, M. Al-Lail, I. Ray and R. B. France, "Specification, Validation, and Enforcement of a Generalized Spatio-Temporal Role-Based Access Control Model," in *IEEE Systems Journal*, vol. 7, no. 3, pp. 501-515, Sept. 2013.

[2] M. Ahmed, A. T. Litchfield, "Taxonomy for Identification of Security Issues in Cloud Computing Environments," in Journal of Computer Information Systems, 58:1, 79-88, 2018.

[3] Asma Alshehri and Ravi Sandhu. 2016. Access control models for cloud-enabled internet of things: A proposed architecture and research agenda. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). IEEE, 530–538.

Acknowledgements

This research was supported by the URG research grant at TAMIU.