RV College of Engineering

EXPERIENTIAL LEARNING
COMPUTER NETWORKS

STORAGE AWARE MECHANISM FOR IoT APPLICATIONS

TEAM:
Rakesh V S[1RV22AI043]
Niranjan M S [1RV22AI067]
Sharankrishna K[1RV22AI051]
Sandeep s p [1RV22AI049]

Go, change the world

RV College of Engineering®

INTRODUCTION

- IoT devices often lack robust security measures, making them vulnerable to cyber threats. We need to understand the challenges in securing IoT data, including limited processing power, diverse communication protocols, and the sheer volume of connected devices.

- In a household environment, data security is critical to protect personal information, prevent unauthorized access, and maintain the functionality of devices. Ensuring data-aware and secure storage mechanisms is essential for safeguarding home IoT networks.

- IoT devices are vulnerable to cyber-attacks due to weak security protocols. Encryption is a crucial component of IoT data security. Various the application in the safeguarding IoT data, implement different encryption techniques and their confidentiality, integrity, and authenticity of information.
- "Data aware system" refers to the capability of the system to understand and manage the data based on its context, sensitivity, and usage requirements. This involves knowing what type of data is being stored, how it should be protected, who should have access to it, and how it should be handled throughout its lifecycle.

RV College of Engineering®

PROBLEM STATEMENT

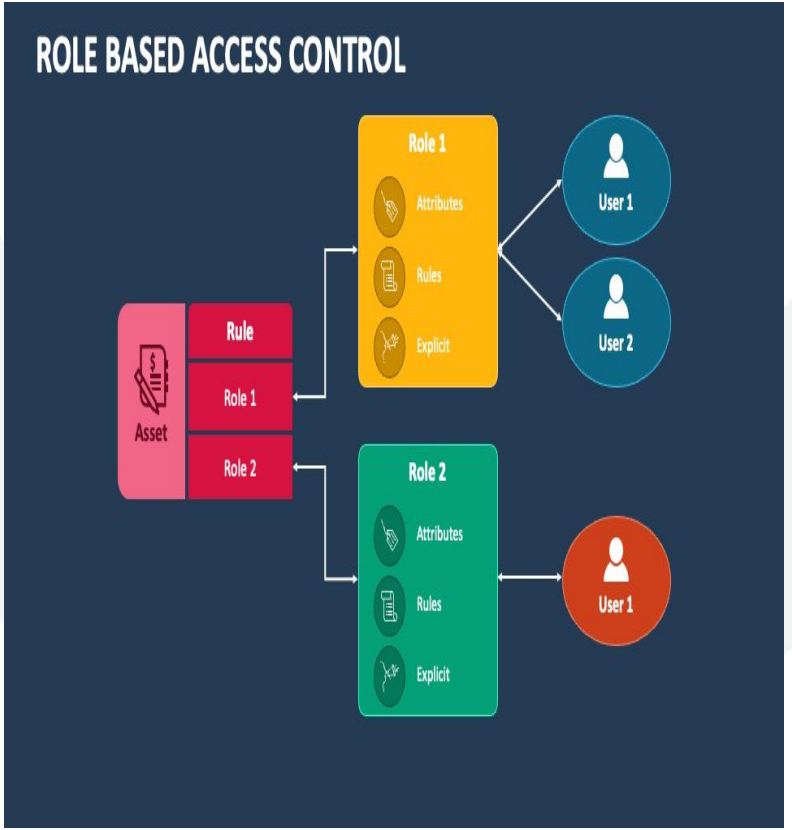
- We aim to develop a mechanism that can store and secure data efficiently for IoT applications in home environment.
- In a home environment, there exists a lot of IoT devices which lead to a complex network hence the vulnerabilities in these devices can be exploited compromising the network security.
- Traditional data storage solutions are insufficient for the dynamic and interconnected nature of IoT systems. We need a scalable, efficient and secure storage solution that is aware of the data context and relationships.

RV College of Engineering®

LITERATURE SURVEY

❖ ROLE BASED ACCESS CONTROL :

- ➢ **Centralized Management**: RBAC simplifies administration by assigning permissions to roles rather than individual users.
- ➢ **Least Privilege Principle**: RBAC ensures users only have access to necessary information and resources for their roles.
- ➢ **Improved Security and Compliance**: RBAC enhances security and helps organizations comply with regulatory requirements.
- ➢ **Scalability and Flexibility**: RBAC is scalable and flexible, easily accommodating organizational changes and growth.



LITERATURE SURVEY

- SELECTIVE DATA UPLOADING:
  - Relevance-Based Selection:

    Only upload data that is relevant or has changed significantly. Use thresholds to determine if new data is sufficiently different from the last upload.
  - Event-Driven Uploading:

    Trigger data uploads only when certain events occur (e.g., temperature exceeds a threshold), rather than uploading data continuously.
  - Sensor Fusion:

    Combine data from multiple sensors to reduce redundancy and overall amount of data needing to be transmitted

RV College of Engineering®

LITERATURE SURVEY

- Graph Databases:
  - Graph databases use a flexible schema that can easily adapt to changes in data structure, which is ideal for IoT environments where new types of devices and data can be introduced frequently.
  - Graph databases excel at managing and querying interconnected data, making them well-suited for IoT applications that involve complex relationships between devices, sensors, and users.

- Hierarchical Multi-domain Network Security Situation Awareness (NSSA):
  - NSSA uses a multi-layered approach to security, where each layer focuses on specific aspects of the network. This hierarchy enhances the ability to monitor and secure diverse and complex IoT environments.
  - Ensures that data collected from IoT devices is accurate, consistent, and protected from unauthorized modifications. This is vital for maintaining trust in IoT systems.

RV College of Engineering®

METHODOLOGY

- Multi-layered architecture inspired by NSSA model:
  - This ensures secure and efficient data storage for home IoT applications.It incorporates multiple layers to handle different aspects of data security and management.
- Basic Security Layer:-
  - The foundational layer responsible for the initial collection, storage, and basic security measures of IoT data (IoT Devices, Data Aggregation, Initial Security Measures).
  - Basic encryption and authentication mechanisms to ensure data integrity and prevent unauthorized access at the device level.
  - It continuously collects data from various IoT devices and does basic filtering and aggregation of data to reduce noise and prepare it for further analysis.

RV College of Engineering®

METHODOLOGY

- Security Analysis Layer:-
  - The intermediate layer responsible for analyzing the aggregated data to detect potential security threats and anomalies (Data Storage, Data Analysis Tools, Security Protocols).
  - Analyze the collected data to identify patterns, trends, and potential security threats and using machine learning algorithms to detect anomalies and unusual behavior in the IoT network.
  - Utilize Neo4j's graph capabilities to map and analyze relationships between different data points, providing a comprehensive view of the IoT ecosystem.
- Threat Intelligence Layer:-
  - The topmost layer responsible for integrating external threat intelligence and providing advanced security insights (Threat Intelligence Feeds, Advanced Analytics, Incident Response).
  - Correlate data from the internal IoT network with external threat intelligence to identify potential risks and generate actionable security insights and recommendations based on the combined analysis of internal and external data.
  - Implement incident response strategies to mitigate detected threats and minimize potential damage.

RV College of Engineering®

METHODOLOGY

- Neo4j graph database:-
  - Used to manage and secure IoT data relationships and interactions effectively.
  - Store IoT data in a graph format, representing devices, data points, and their interactions as nodes and edges.
  - Use Cypher query language to perform complex queries and analysis on the graph data, identifying patterns and potential security threats.
- Core components of the Data model:-
  - Nodes:-
    - IoT devices(`device_id`, `device_type`, `location`, `status`, and `last_active_timestamp`),
    - Users(`user_id`, `name`, `role`, and `access_level`),
    - Network components(`component_id`, `component_type`, `ip_address`, and `status`),
    - Security events(`event_id`, `event_type`, `timestamp`, `description`, and `severity`).
  - Labels:- DEVICE, USER, NETWORK, SECURITY_EVENT.
  - Properties: Device ID, type, user details, event timestamps.
  - Relationships: CONNECTS_TO, BELONGS_TO, GENERATES.

RV College of Engineering®

METHODOLOGY

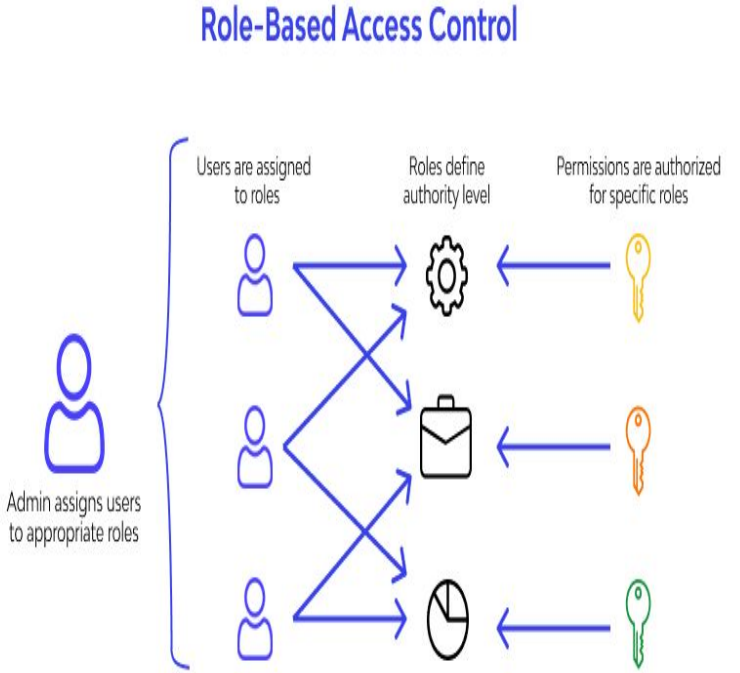
- Example:-

```
// Create nodes
CREATE (device1:DEVICE {id: 'device1', type: 'sensor', location: 'living room'})
CREATE (user1:USER {id: 'user1', name: 'Alice'})
CREATE (network1:NETWORK {id: 'network1', type: 'WiFi', ssid: 'HomeNetwork'})

// Define relationships
CREATE (device1)-[:BELONGS_TO]->(user1)
CREATE (device1)-[:CONNECTS_TO]->(network1)

// Add security event
CREATE (event1:SECURITY_EVENT {id: 'event1', type: 'login_attempt', timestamp: '2024-07-
CREATE (device1)-[:GENERATES]->(event1)

// Query example: Find all devices belonging to a specific user
MATCH (u:USER {id: 'user1'})-[:BELONGS_TO]-(d:DEVICE)
RETURN d
```

RV College of Engineering®

METHODOLOGY

- Using Role-based access control (RBAC) to restrict data access based on user roles, ensuring that only authorized personnel can access sensitive data.
- For example:-
  - Roles include Admin, Special User, Standard User, and Guest.
  - Admins have full access, Special Users have elevated access with some restrictions, Standard Users have basic access, and Guests have minimal access.
  - Implement checks in the application to enforce RBAC policies, ensuring that users can only perform actions permitted by their role.
- Encrypting data stored in databases and file systems using AES-256 encryption (Data at rest). Using TLS to encrypt data transmitted over the network, ensuring secure communication between IoT devices, gateways, and the central storage system (Data in transit).
- Implementing a robust key management system (KMS) to securely store and manage encryption keys. Rotating keys periodically and using hardware security modules (HSMs) for added security.



RV College of Engineering®

CONCLUSION

- The proposed system ensures that all data collected from IoT devices is stored securely, protecting it from unauthorized access and tampering. Implementing role-based access control (RBAC) restricts access to data based on user roles, minimizing the risk of data breaches.
- Using a graph database like Neo4j allows for efficient handling of complex, interconnected data typical of IoT environments. It supports dynamic data modeling, accommodating changes and new data types without significant reengineering.
- The system is designed to scale horizontally, distributing data across multiple nodes to handle increasing volumes of IoT data. This ensures high availability and performance even as the number of connected devices grows.

RV College of Engineering®

REFERENCES

- GX. Xiaoling and Y. Liu, **"Graph Database Based Network Security Situation Awareness Data Storage Method,"** in *Proceedings of the International Conference on Network and System Security (NSS)*, vol. 1, no. 1, pp. 123-130, 2020. doi: 10.1007/978-3-030-56229-6_10.
- J. Doe, A. Smith, and B. Lee, **"A Private and Efficient Mechanisms for Data Uploading in Smart Physical Systems,"** in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3245-3253, June 2019. doi: 10.1109/TII.2019.2902345.
- M. Brown, L. Green, and R. Black, **"Collective Data Sanitization for Preventing Sensitive Information Inference Attacks in Social Networks,"** in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1271-1283, May 2019. doi: 10.1109/TIFS.2019.2901427.
- P. White, Q. Zhou, and Y. Zhang, **"Multi-Sensor Data Fusion for Cyber Security Situation Awareness,"** in *IEEE Access*, vol. 8, pp. 123456-123465, 2020. doi: 10.1109/ACCESS.2020.2985678.
- T. Johnson and S. Wang, **"A Situation Awareness Model for Information Security Management,"** in *Computers & Security*, vol. 85, pp. 123-133, 2019. doi: 10.1016/j.cose.2019.04.010.