International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 10 | Oct 2025 www.irjet.net p-ISSN: 2395-0072

A Context-Aware Access-Control Framework for Securing Distributed IoT Environments

Diaeldin Izeldin Mohamed[1], Dr. Sally D. Abualgasim[2], Dr. Yasir Abdelgadir Mohamed[3]

[1] *University of Gezira, Faculty of Engineering and Technology, Wad-Medani, Sudan*
[2] *University of Gezira, Faculty of Engineering and Technology, Wad-Medani, Sudan*
[3] *A'Sharqiyah University, College of Business Administration/MIS, Ibra, Oman*

Abstract –

As Internet of Things (IoT) ecosystems expand across distributed and heterogeneous environments, ensuring fine-grained, adaptive, and context-aware access control has become essential for maintaining trust, confidentiality, and resilience. This paper presents a comprehensive access-control framework that integrates environment analysis, dynamic policy enforcement, and defense-in-depth strategies to safeguard IoT resources from both conventional and emerging threats. The proposed model is built upon classical access-control principles so as to extend functionality through real-time contextual evaluation, multi-layer firewall integration, and adaptive authorization mechanisms. Virtualization and policy-driven automation enable multi-domain deployments, decision accuracy, and administrative efficiency. Experimental validation in a simulated IoT environment shows that the proposed solution managed to reduce unauthorized activities, similarly, offers low access latency, and improves dependability over current IoT access-control techniques. Furthermore, the results confirm the framework's scalability and its ability to dynamically adjust to evolving network conditions and threat landscapes. This study contributes with a practical and extensible solution so as to secure IoT infrastructures while providing a foundation for future research in intelligent and self-adapting access-control architectures.

Keywords: *Internet of Things, Access Control, Dynamic Authorization, Context-Aware Security, Distributed Resources.*

1. INTRODUCTION

The Internet is rapidly evolving from a communication medium connecting human users into a globally interconnected ecosystem of intelligent devices [1]. Rather than functioning as a static network of terminals, future architectures will comprise pervasive systems of sensors, actuators, and embedded electronic components that collectively form the Internet of Things (IoT) [1]. These devices, seamlessly integrated into everyday objects and environments, enabling continuous interaction between the physical and digital realms, and supporting a wide range of applications in many areas, such as healthcare, industry, and smart cities. However, this transformation introduces substantial security and privacy challenges. A lot of IoT nodes are thought to be resource-constrained, which means they may not have the computing power or storage space so as to employ standard encryption and authentication methods [2]. Furthermore, the extreme heterogeneity of devices, their dynamic operating conditions, and the massive scale of deployment render traditional access control approaches inadequate for protecting modern IoT infrastructures [3]. These limitations draw the attention to the necessity for a context-aware, adaptive, and lightweight access-control framework capable of maintaining trust, integrity, and availability in dynamic, distributed environments [4].

1.1 Security and Privacy Challenges in IoT

Some of the key challenges in securing IoT systems include:

- A constrained devices authentication [5].
- Trust establishment among untrusted components [6],
- Detection of rogue nodes [7] [8],
- Privacy protection for user data[9],
- Intrusion detection [10],
- Data integrity and protection [5],
- Access control in dynamic, distributed contexts [11],
- Other issues, such as key management and data aggregation [12].

1.2 Access Control in IoT

Access control serves as an essential block of information security, that is by defining and regulating which entities are authorized to perform specific actions on system resources, such as devices, data, or services. In the context of the Internet of Things (IoT), access control ensures that only trusted and authenticated entities can interact with devices or access sensitive information, thereby fostering trust among interconnected participants However, to implement an effective access control in IoT environments is commonly considered a challenge, that is because of the scale, resource limitations, and distributed nature of these systems [13] [14]. IoT networks often encompass thousands of heterogeneous devices with varying computational capabilities, communication protocols, and security

requirements. These constraints limit the feasibility of traditional access control models—such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC)—which typically rely on centralized policy management and intensive computational processing [13].

Furthermore, delegation of access rights is frequently required in large-scale IoT deployments to maintain operational flexibility and support dynamic interactions among devices, users, and services. To manage such type of delegations in a secure manner across multiple domains will add complexity, especially when devices are intermittently connected or operate autonomously [15] [16]. These challenges highlight the need for frameworks that have lightweight, context-aware, and adaptive access-control features and capable of evaluating contextual parameters in a dynamic manner such as device trust levels, environmental conditions, and behavioral patterns to ensure secure and resilient IoT operations.

1.3 State of the Art

Access control has changed over the recent years, from Discretionary Access Control (DAC) and Mandatory Access Control (MAC) to Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). Researchers have also explored beyond, to History-Based Access Control (HBAC), Relationship-Based Access Control (ReBAC), and Usage Control (UCON). But most of these models fall short in dynamic, open IoT environments. For example, ABAC lacks support for provenance metadata; RBAC suffers from role explosion; UCON introduces ongoing obligations that IoT devices may not support.

In large dynamic systems, manual policy management becomes infeasible. Closed environments might manage that, but IoT's open and dynamic setting demands automated, scalable access control solutions [17] [18].

1.4 Problem Statement and Objectives

The rapid proliferation of Internet of Things (IoT) applications has been hindered by persistent concerns over trust, privacy, and security. The lack of reliable access-control mechanisms in distributed IoT environments has significantly limited users' confidence in adopting IoT-based services. Surveys consistently indicate that a considerable portion of users distrust organizations handling their personal and sensor data, which in turn slows the growth of IoT ecosystems. This study aims to (1) develop a formal framework for modelling access-control entities in open IoT environments so as to reduce manual administrative efforts, (2) design a generic and adaptive model to mitigate security threats and present policy definition in a simpler way, and (3) implement automated delegation, revocation, and verification of access rights across distributed contexts. Rest of paper is organized as follows: Section 2 reviews relevant work, Section 3 explains the access-control architecture, Section 4 implements it, Section 5 analyses experimental findings, and Section 6 closes with future research.

2. RELATED WORK

Access control within Internet of Things (IoT) environments has drawn an attention of researchers as of the growing need for secure and context-aware management of connected devices. The current frameworks generally fall into three main categories: role-based, attribute-based, and context-aware models. Role-Based Access Control (RBAC) simplifies permission assignment by grouping users under predefined roles [19]; however, it lacks flexibility in dynamic IoT settings where device interactions frequently change. Attribute-Based Access Control (ABAC) extends this flexibility as it incorporates user and environmental attributes into policy decisions [20]. To this point, ABAC systems are computationally intensive and struggle to operate efficiently on resource-constrained IoT nodes.

Context-aware access-control frameworks have been introduced so as to overcome the limitations of static models, by integrating contextual information such as device location, network conditions, and behavioral patterns into authorization decisions [21]. While these models improve adaptability, their reliance on predefined contextual parameters limits their responsiveness to rapidly evolving security threats.

Recent research has also explored hybrid access-control architectures which merge centralized decision-making with decentralized enforcement [22] [23], with the aim of balancing scalability and performance. Blockchain-based approaches [24] [25] have further enhanced transparency and trust in distributed IoT environments, however, they still introduce significant latency and storage overheads that hinder real-time enforcement. In a similar way, AI-driven access-control mechanisms have emerged to support threat detection and anomaly prediction [26]; however, most of these efforts focus on theoretical frameworks or small-scale simulations rather than integrated, enterprise-level implementations.

Despite these advances, a significant gap remains in the integration of real-time threat intelligence into the access-control decision loop. Most frameworks operate reactively—evaluating access requests based solely on static policy conditions—without leveraging continuous malware analytics or adaptive rule refinement. This limitation restricts their ability to reflect dynamic responsiveness to zero-day attacks and emerging threat vectors.

In order to address these deficiencies, this study aims to introduce a framework that integrates aspects such as policy-driven, hybrid access-control framework that combines Cisco Advanced Malware Protection (AMP) for threat analysis, Qualys for vulnerability assessment, Cisco Identity Services Engine (ISE) for dynamic policy

enforcement, and Active Directory (AD) for identity verification. This integrated design will have the capability to enable real-time synchronization between device posture assessment and authorization decisions, thus, it bridges the gap between static policy enforcement and adaptive, intelligence-driven access control.

3. PROPOSED FRAMEWORK DESIGN

3.1 Overview

This section outlines the systematic methodology we have adopted so as to design and implement a secure and adaptive Access Control Framework (ACF) for open Internet of Things (IoT) environment. The framework is built upon the classical access-control architecture, integrating contextual intelligence, defense-in-depth mechanisms, and dynamic policy enforcement. The methodology includes environment analysis, framework feature identification, access control information (ACI) modelling, policy establishment, and multi-layered defense integration.

3.2 Framework Design Process

1) The research methodology adopts the following structured multi-phase approach:

   a. The IoT ecosystem was studied so as to identify distributed resources, communication channels, and the heterogeneity of connected devices (e.g., sensors, gateways, servers).

   b. The core features of the proposed framework were derived, emphasizing scalability, adaptability, delegation, and fine-grained access control.

   c. Access control entities (for example: initiators, targets, access requests, and contextual attributes) were defined and structured based on the ISO/IEC X.800 model.

   d. Rule-based and identity-based access control policies were developed for different IoT architectures (service-based, client-based, end-to-end, and centralized).

2) Layered network security components—core network security, perimeter security, communication security, and endpoint protection—were incorporated to mitigate internal and external threats.

To operationalize the Access Decision Function (ADF), the framework incorporates a hierarchical decision workflow that evaluates each access request against multiple layers of policies. As illustrated in Fig -1, the process starts with a preliminary check against the default access control policy so as to detect known threats. If no immediate threat is identified, the request is assessed through identity-based policies and, subsequently, mapped to the appropriate category of initiator (service-based, centralized, client-based, or end-to-end). Each branch enforces tailored access control rules, at the time, the non-matching or untrusted requests will be by default denied. This flowchart highlights the adaptive nature of the framework, this will ensure both proactive threat mitigation and fine-grained access management in distributed IoT environments.

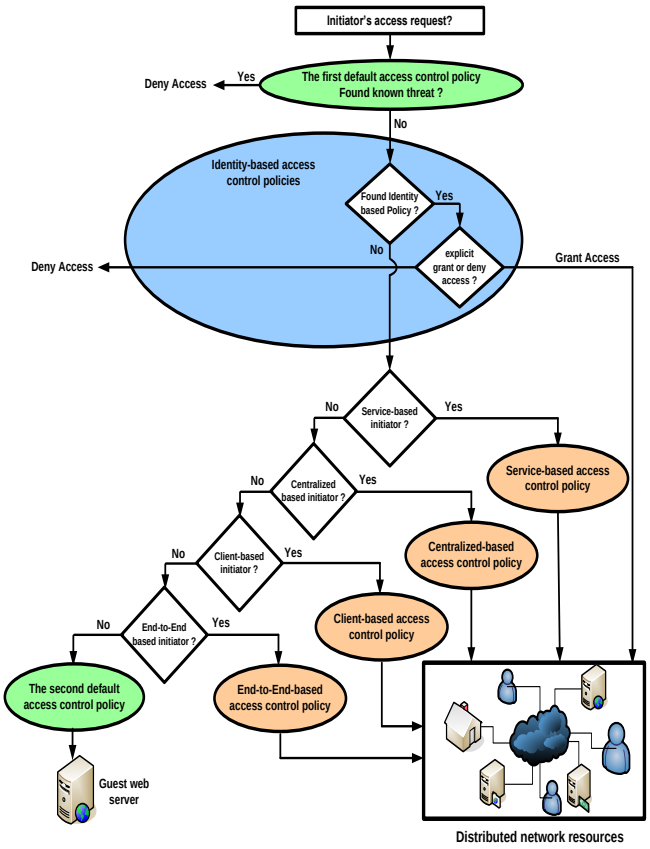

Fig -1: Overall Framework Design

3.3 Access Control Policy Representation

The framework incorporates two default policies and four specialized rule-based policies designed for diverse IoT architectures.

- Automatically enforced so that it prevents common attacks such as IP spoofing, DoS, ICMP flooding, and unauthorized access to unused ports.
- Custom-defined for service-based, client-based, end-to-end, and centralized configurations to ensure adaptive security in dynamic environments.
- Updated periodically so as to reflect user-specific privileges and evolving organizational security requirements.

3.4 Access Control Information (ACI) Representation

The ACI model captures the essential attributes for decision-making, classified into:

- Initiator ACI: Entity identifiers, group affiliations, and sensitivity markings.
- Target ACI: Resource identifiers, container contexts, and security classifications.
- Access Request ACI: Operation type, integrity level, and data sensitivity.
- Contextual ACI: Real-time environmental data such as time, location, and detected threats.

3.5 ACI Binding and Protection

Each ACI is bound to its respective entity using cryptographic techniques so as to ensure the authenticity and integrity of exchanged control information, e. The Network Access Device (NAD) interacts with the RADIUS and Domain Controller (DC) to authenticate and enforce access decisions. All ACI exchanges are digitally signed or encapsulated within security tokens to prevent tampering or replay attacks during transmission.

3.6 Defense-in-Depth Architecture

The proposed framework applies a multi-layered defense architecture (Fig -2) that reinforces security across four levels:

- Managed by a Domain Controller integrating DNS, authentication, VPN, and certificate authority services.
- Dual-firewall topology employing a Perimeter Firewall Host and Zone-Based Firewall Host, so as to mitigating external attacks and isolating internal network zones.
- All transmissions are protected using AES-128 encryption for service-based communications, VPN tunnelling for client-based users, and IPSec VPN for end-to-end secure links.
- Automated endpoint configuration ensures uniform protection, complemented by optional user-controlled measures such as screen locking and one-time passwords (OTPs).

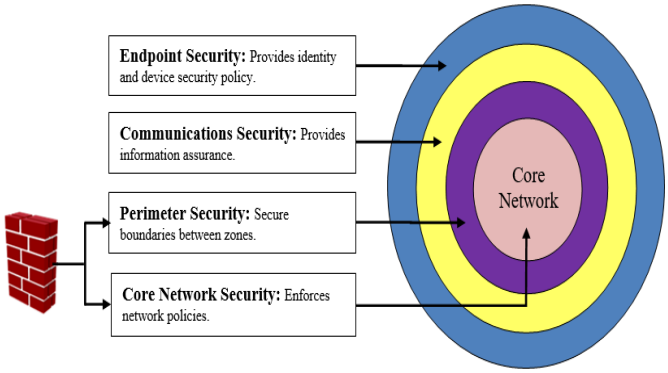

Fig -2: A Multi-Layered Defense Architecture

3.7 Context-Aware Authorization Mechanism

Fig –3 shows the designed Context Authentication and Authorization (CAA) Framework. It was implemented using Cisco Identity Services Engine (ISE) integrated with Active Directory (AD), Cisco Advanced Malware Protection (AMP) and Qualys-Common Vulnerability Scoring System (Qualys-CVSS).

- The ISE dynamically adjusts access privileges based on contextual inputs (device posture, location, time, and threat intelligence).
- Real-time data from Posture Validation Servers (PVS) informs adaptive policy enforcement.
- Access privileges automatically degrade or elevate depending on vulnerability score (e.g., medium score vulnerable device results in reduced authority).

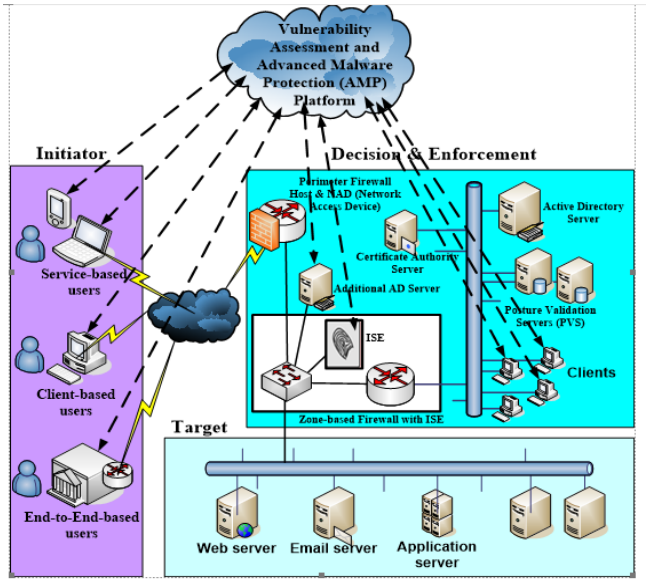

Fig -3: Context-aware access control architecture integrating ISE, AD, and AMP.

3.8 Interaction Workflow

As illustrated in Fig -4, the access control sequence proceeds as follows:

1) The Initiator submits an access request through the perimeter firewall host and NAD.

2) The perimeter firewall host enforces the default access control policies to mitigate most the known security threats then, forward the request to the ISE.

3) The ISE retrieves contextual and posture data from the PVS.

4) The ISE communicates with the active directory server to validate the initiator's identity. If it is valid, ISE requests the initiator's access control information (ACI).

5) According to the ACI, policy sets, and the initiator's health state, the ISE makes the access control decision and send it to the NAD.

6) The NAD enforces the access control decision with the initiator.

7) The initiator is allowed/denied to access the designated target resources.

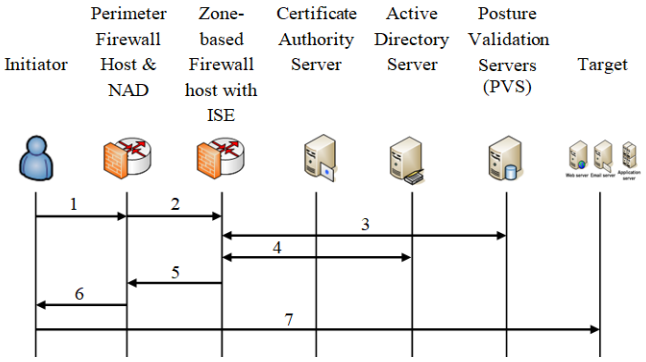

Fig -4: Sequential access control workflow in the proposed framework

3.9 Policy Evaluation Logic

ISE's policy evaluation engine processes access requests through predefined policy sets:

- Each request is evaluated against contextual, identity, and threat-based conditions.
- If authentication and authorization conditions are satisfied, then the access will be granted; otherwise, denied automatically.
- Policies are modular and reusable, enabling automated handling of new IoT users without manual configuration.

As a summary to this; the proposed methodology provides a structured and scalable approach to IoT access management by combining formal policy definition, contextual adaptation, and defense-in-depth protection. The framework achieves real-time threat-aware decision-making, low administrative overhead, and strong resilience against evolving IoT threats, this by utilizing Cisco ISE, AMP, Qualys, and AD integration.

4. IMPLEMENTATION

4.1 Access Control Framework Implementation

- The proposed access-control framework (Fig -3) was implemented using a hybrid setup combining physical and virtualized components so as to ensure robust, scalable, and secure access management across a distributed IoT environment.
- A dedicated server acted as the centralized authentication and policy authority, enforcing uniform security rules and user authentications. This will ensure that all access requests were verified against a unified directory service, thereby minimizing unauthorized access.
- Layer-3 Switch as Network Access Device (NAD) is configured as the Access Enforcement Function (AEF), the Layer-3 switch handled routing, switching, and enforcement of access decisions made by the Access Decision Function (ADF).
- The perimeter router was configured as a VPN server to establish secure tunnels for remote users. It also enforced the first default access-control policy to mitigate threats at the network entry point.
- Cisco ISE was used as the Access Decision Function to evaluate real-time contextual data and apply dynamic policies. It provided threat-centric access control and centralized policy management.
- Ten simulated client nodes were used so as to emulate user requests and test performance under realistic IoT network loads.

As shown in Fig -5, the implementation was performed in a virtualized environment using VMware ESXi 6.0 on an HP ProLiant DL380 G7 server (12-core Intel® Xeon® CPU, 51 GB RAM). The ESXi hypervisor hosted multiple virtual machines, including Windows Server 2012 (Active Directory) and Cisco ISE routers. This configuration enabled efficient resource management, rapid reconfiguration, and replication of complex IoT architectures.

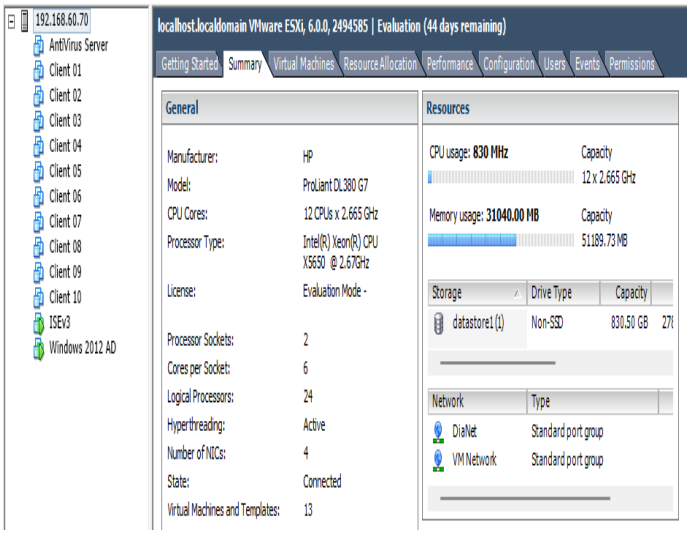

Fig -5: VMware virtualized implementation environment

4.2 Active Directory and Organizational Structure

The domain controller (dia.com) was structured into four Organizational Units (OUs) representing distinct IoT architectural domains as shown in Fig -6:

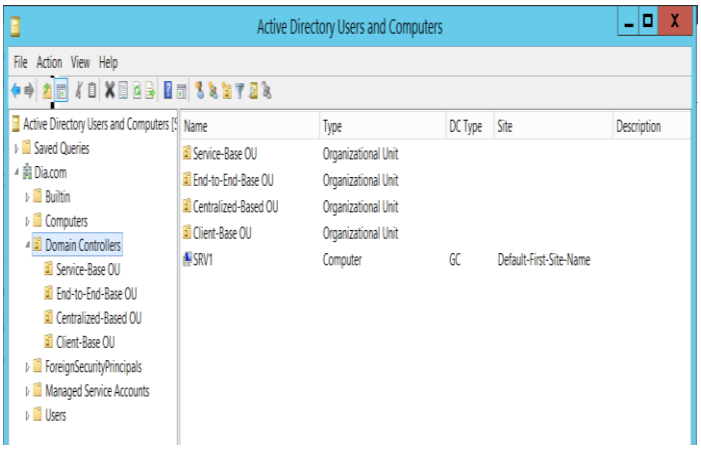

Fig -6: Four Organization Units that Represent the IoT Architectures

- The Service-based OU managing service-oriented devices and applications.
- End-to-End OU securing full-path device-to-device communications.
- Centralized OU enforcing top-level control and unified policy management.
- Client-based OU isolating end-user devices with tailored permissions.

This logical segmentation supported fine-grained policy enforcement and scalability so as to achieve distributed IoT deployments.

4.3 Security Component Configuration

- The Certificate Authority (CA) Server Configured for automatic certificate issuance to internal users and manual web enrollment for remote users.
- Authentication Server: Implemented Multi-Factor Authentication (MFA) combining password, token, and biometric validation so as to strengthen user identity assurance.
- Cisco Advanced Malware Protection (AMP) and Qualys continuously assessed device integrity and synchronized threat intelligence with ISE for proactive vulnerability management.
- The ISE server (ISE3.dia.com – 192.168.60.65) was configured with:
  - Threat-Centric NAC (TC-NAC): real-time access adaptation based on threat severity.
  - Integration of Cisco AMP in conjunction with vulnerability assessment tools (Qualys): third-party validation of endpoint health.
  - Connection to AD Source (dia.com): identity-based policy enforcement.
  - Network Access Device (NAD) Configuration: using Cisco Switch 3750 for policy enforcement as shown in Fig -7.

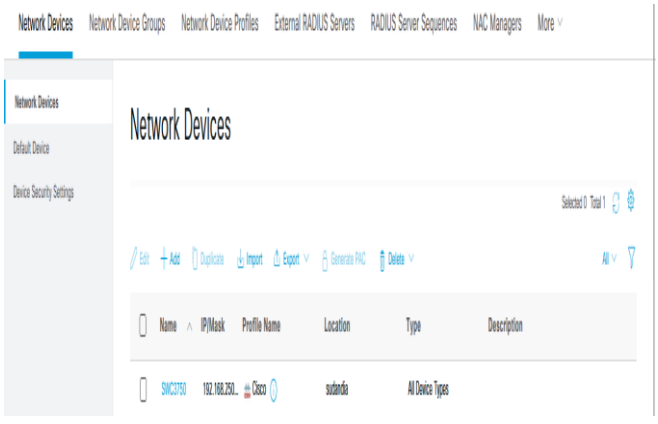

Fig -7: Network Access Device (NAD)

ISE policy sets were created to define conditions, authentication, and authorization policies for different access categories.

5. RESULTS AND ANALYSIS

Cisco AMP identified device vulnerabilities, health status, and root-cause analyses for detected threats. These metrics enhanced visibility of endpoint compliance, ensuring up-to-date patching and anti-malware integrity.

As illustrated in Fig -8, the summary provides an overview of the status of client devices within the network. This summary includes critical metrics such as the total number of clients, the number of devices that require antivirus (AV) updates, those that need an update for the Cisco AMP connector, and other relevant statuses.

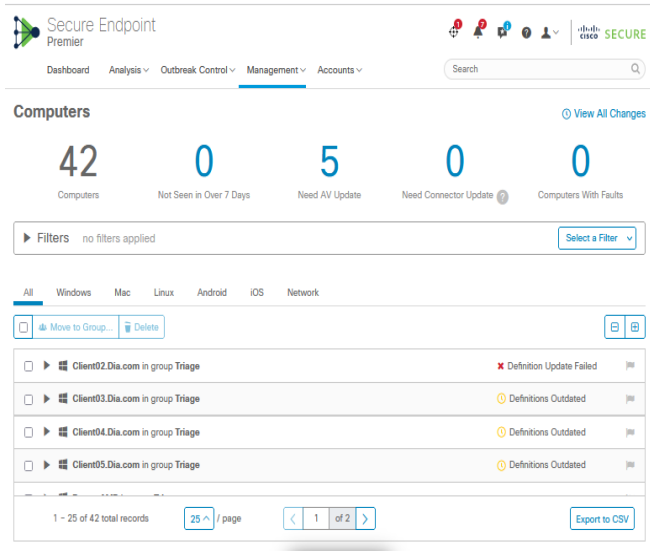

Fig -8: The Status of Client Devices within The Network

Fig -9 shows the threats root cause analysis. These metrics offer valuable insights into the security compliance of client devices, helping administrators identify and address potential vulnerabilities proactively.

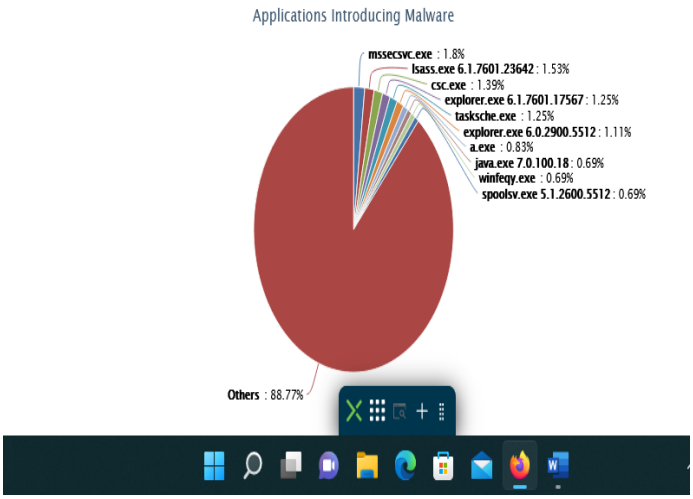

Fig -9: Threats Root Cause Analysis

ISE live logs (as shown in Fig -10) recorded detailed the Access Decision process under varying policy conditions:

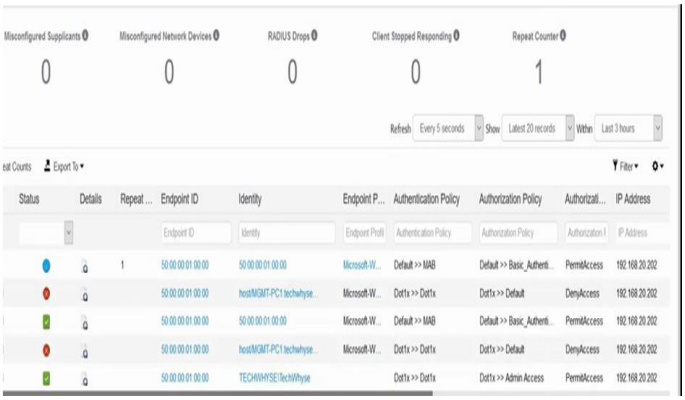

Fig -10: ISE live logs

- Access Granted under Default Policy Set using MAB + Basic_Authentication.
- Access Denied under Dot1x Policy Set requiring stricter IEEE 802.1X authentication.
- These findings validated the system's ability so as to enforce differential policy decisions dynamically.

The results confirm full attainment of the study's objectives:

a) The proposed model reduced administrative overhead by automating policy definition and access verification.

b) Integration of ISE and Cisco AMP in conjunction with Qualys achieved real-time contextual enforcement, improving threat response and scalability.

c) The framework successfully automated delegation, revocation, and validation of access rights using Qualys-CVSS.

6. CONCLUSION AND FUTURE WORK

This study presented the design, implementation, and evaluation of a context-aware access control framework tailored so as to achieve these goals in distributed Internet of Things (IoT) environments. The proposed framework successfully integrated core security components—Domain Controller, Cisco Advanced Malware Protection (AMP), Qualys, and Cisco Identity Services Engine (ISE)—to deliver fine-grained, scalable, and adaptive access management.

Experimental results demonstrated that the framework effectively mitigates unauthorized access, streamlines policy definition, and automates delegation and revocation in distributed contexts. These outcomes confirm the framework's ability to balance security robustness with

administrative efficiency, achieving all research objectives while addressing the dynamic security demands of IoT ecosystems.

Although the framework achieved strong performance within the simulated testbed, scalability and performance under very large or heterogeneous IoT environments were not fully explored, but should be considered in the future. Additionally, real-world deployment are expected to reveal operational and interoperability challenges that extend beyond the controlled experimental setup.

Future research should focus on and incorporate evaluating performance in large-scale and heterogeneous IoT systems, integrating artificial intelligence and machine learning for predictive threat detection and adaptive policy generation, and testing the framework's applicability across different industry sectors so as to refine its generalizability and efficiency.

All in all, the proposed access-control framework provides a practical and extensible foundation so as to securing next-generation IoT systems. It highlights the importance of combining contextual intelligence, multi-layer defense, and policy automation to safeguard interconnected environments while minimizing administrative complexity.

7. REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sept. 2013, doi: 10.1016/j.future.2013.01.010.

[2] O. Garcia-Morchon, S. Kumar, and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges," *RFC 8576*, Apr. 2019, doi: 10.17487/RFC8576.

[3] R. Xu, Y. Chen, E. Blasch, and G. Chen, "A Federated Capability-based Access Control Mechanism for Internet of Things (IoTs)," in *Sensors and Systems for Space Applications XI*, Proc. SPIE, vol. 10641, 2018, doi: 10.1117/12.2305619.

[4] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N. B. Carvalho, "Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment," *Sensors*, vol. 20, no. 22, art. 6420, Nov. 2020, doi: 10.3390/s20226420.

[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008

[6] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951

[7] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.

[8] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, Jan. 2010, doi: 10.1016/j.clsr.2009.11.008.

[9] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, Jan. 2018, doi: 10.1016/j.future.2017.07.060.

[10] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of security services in IEEE 802.11 wireless networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 1, pp. 4–30, Jan. 2012, doi: 10.1002/wcm.975

[11] X. Ma, F. Fang, and X. Wang, "Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks," *arXiv*, Jan. 2025. [Online]. Available: https://arxiv.org/abs/2501.03601

[12] K. Srinivas and S. Kadapa, "Secure key management techniques in IoT-enabled wireless sensor networks," *AIP Conference Proceedings*, vol. 2971, no. 1, 2024. doi: 10.1063/5.0195860

[13] S. A. Alhoori, "Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions," *Sensors*, vol. 23, no. 4, art. no. 1805, Feb. 2023, doi: 10.3390/s23041805.

[14] H. Filho, "A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art," *MDPI Electronics*, vol. 6, no. 1, art. 9, Jan. 2023, doi: 10.3390/electronics6010009.

[15] R. Xu, Y. Chen, E. Blasch, and G. Chen, "A Federated Capability-based Access Control Mechanism for Internet of Things (IoTs)," *arXiv preprint arXiv:1805.00825*, May 2018. (Preprint)

[16] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A Blockchain-Enabled Decentralized Capability-Based Access Control for IoTs," *Future Generation Computer Systems*, vol. 124, pp. 350–364, 2021, doi: 10.1016/j.future.2021.05.011.

[17] S. Alharbi, S. Basudan, and H. Wang, "A Survey on Access Control for the Internet of Things," *Future Internet*, vol. 14, no. 6, art. 165, Jun. 2022, doi: 10.3390/fi14060165.

[18] T. Rehman, K. Grønbæk, and M. Abdullah, "Adaptive Context-Aware Access Control for IoT Environments Leveraging Fog Computing," *International Journal of Information Security*, 2024, doi: 10.1007/s10207-024-00866-4

[19] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Access Control in the Internet of Things: Big Challenges and New Opportunities," *Computer Networks*, vol. 112, pp. 237–262, Jan. 2017, doi: 10.1016/j.comnet.2016.11.003

[20] H. Hu, G.-J. Ahn, and K. Kulkarni, "Anomaly discovery and resolution in attribute-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 17, no. 4, pp. 1–41, Apr. 2015, doi: 10.1145/2675131

[21] D. Ouaddah, A. Ait Ouahman, and A. Abou Elkalam, "Towards a Context-Aware Access Control Model for Smart Environments," *Journal of Information Security and Applications*, vol. 38, pp. 53–65, Feb. 2018, doi: 10.1016/j.jisa.2017.11.008

[22] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 726–739, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.011.

[23] S. Pal and Z. Jadidi, "Protocol-Based and Hybrid Access Control for the IoT: Approaches and Research Opportunities," *Sensors*, vol. 21, no. 20, art. no. 6832, Oct. 2021, doi: 10.3390/s21206832

[24] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.

[25] S. Cha, J. Kim, and J. H. Park, "Blockchain-based Access Control for IoT: Challenges and Future Directions,"*Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5521876, doi: 10.1155/2021/5521876

[26] R. S. T. Lee, S. M. Zaki, and S. Y. Lee, "AI-Driven Access Control and Anomaly Detection in Internet of Things Networks: A Survey," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 1736–1751, Sep. 2022, doi: 10.1109/TNSM.2022.3189956