Mohamed Ayari[1,2]
Atef Gharbi[1]
Yemen El Touati[1]
Zeineb Klai[1,3]
Akil El Kamel[3]
Abdulsamad Yahya[1]

Enhancing Security in IoT Networks: A Focus on Authentication and Access Control

Abstract - This research paper addresses the escalating security concerns within the Internet of Things (IoT) by focusing on authentication and access control mechanisms. We explore various challenges unique to IoT, such as scalability and device diversity, and review both traditional and advanced security measures. The paper highlights innovative authentication techniques and access control models like RBAC and ABAC, demonstrating their effectiveness through practical case studies in sectors like healthcare and smart home technology. The main contribution is the presentation of tailored security strategies that ensure robust protection for IoT networks against current and future threats, paving the way for safer IoT implementations

Keywords: IoT Security; Authentication; Access Control; Data privacy; Encryption; Smart Devices Security.

I. Introduction

The Internet of Things (IoT) has drastically changed how we interact with technology, blending the digital and physical realms and transforming various sectors. As IoT technology becomes more embedded in critical infrastructure, robust security frameworks, especially around authentication and access control, become crucial. This paper provides a comprehensive analysis of recent developments and ongoing challenges in the field of IoT security.

IoT systems exhibit inherent vulnerabilities due to their distributed nature, which are exploited in numerous cyber-attacks. This complex security landscape requires sophisticated authentication mechanisms to verify device and user identities effectively. The importance of robust authentication systems in IoT is emphasized in studies by Mendez and Papapanagiotou, who discuss the layered security approaches necessary for protecting IoT infrastructures [1-2]. Similarly, Pectu, et. Al., explore how blockchain technology can be utilized to provide decentralized and secure authentication solutions [3].

In addition to authentication, access control is pivotal in ensuring that only authorized entities have access to specific data and actions. Abie (2021) highlights the necessity of adaptive security models that respond dynamically to perceived risks and threats in IoT systems [4]. These models benefit from advancements in artificial intelligence and machine learning, which can detect anomalous behavior and enforce security policies automatically, as outlined by Xu, H. et al. (2023) [5].

Technological innovations continue to influence IoT security strategies. Pal, Dorri, and Jurdak (2022) argue that blockchain can enhance privacy and security across IoT devices by creating transparent and tamper-proof systems for managing identities and access controls [6]. Furthermore, the integration of AI in monitoring and responding to security threats is detailed by Yaseen (2023), who discusses the deployment of AI-driven intrusion detection systems [7].

[1]*Faculty of Computing and Information Technology, Northern Border University –Kingdom of Saudi Arabia,*
[2]*Syscom Laboratory, National Engineering School of Tunis, University of Tunis El-Manar, Tunisia*
[3]*Faculty of Sciences of Sfax, University of Sfax, Tunisia*
mohamed.ayari@nbu.edu.sa
atef.gharbi@nbu.edu.sa
yamen.touati@nbu.edu.sa
Zeineb.klai@nbu.edu.sa
akil.elkamel@nbu.edu.sa
Abdulsamad.qasem@nbu.edu.sa

However, the evolution of IoT also presents new challenges. As Coiduras et al. (2014) point out, privacy concerns are increasingly significant as more personal data is collected and processed by IoT devices [8]. These issues are compounded by the scalability of IoT networks, where managing security configurations across millions of devices becomes untenable without automated systems.

Regulatory and standardization efforts are also crucial in shaping IoT security. Kabir and Alam (2023) discuss the impact of international regulations on IoT security standards, emphasizing the need for consistent and enforceable policies worldwide [9]. Such regulations not only help mitigate risks but also standardize security practices across industries.

Looking forward, the field of IoT security is set to evolve with technological advancements. The development of more resilient cryptographic solutions, as discussed by Varzaneh et al.(2024), is critical in protecting against sophisticated cyber threats [10]. Similarly, the potential for predictive security measures that preemptively address vulnerabilities before they are exploited is being researched, with promising implications for the future of IoT security.

The security of IoT systems is a multifaceted issue that involves complex interactions between technological solutions, regulatory frameworks, and the continuous evolution of cyber threats. The referenced works provide a broad overview of the current state and future directions of IoT security, emphasizing the critical role of advanced authentication and access control mechanisms in securing IoT ecosystems. The paper is organized into six main sections for a systematic exploration of the topic: Section 1 introduces the concept of IoT and outlines its significant security challenges; Section 2 discusses various authentication mechanisms tailored for IoT; Section 3 examines the different models of access control suitable for IoT environments; Section 4 focuses on technological advancements, such as blockchain and AI, that enhance IoT security; Section 5 analyzes the impact of regulatory frameworks on IoT security measures; and Section 6 concludes with a synthesis of the key findings and future research directions. This structure provides a clear pathway through the complexities of IoT security, ensuring a comprehensive analysis from fundamental concepts to advanced applications.

II. Understanding IoT Security Challenges

The exponential growth of the Internet of Things (IoT) brings with it an array of benefits and conveniences across industries and personal applications. However, this expansion also introduces substantial security risks that must be carefully managed to protect sensitive data and maintain system integrity. This section delves into the unique security challenges inherent to the IoT ecosystem and discusses the crucial roles of authentication and access control in mitigating these risks.

A. Security Concerns Specific to IoT

IoT environments are inherently complex due to their extensive and varied nature. Key security concerns that are particularly pronounced in the IoT landscape include:

1. **Diversity of Devices and Protocols**: IoT networks incorporate a wide range of devices, each potentially operating on different platforms and communication protocols. This diversity complicates the implementation of a unified security strategy and increases the potential attack surface.
2. **Resource Constraints**: Many IoT devices are designed to be cost-effective and energy-efficient, which often means they have limited processing power and memory. This constraint restricts the ability of these devices to handle advanced encryption and other security processes.
3. **Scalability**: IoT networks are scalable and can quickly grow to include thousands or even millions of interconnected devices. Each new device potentially introduces new vulnerabilities, making scalable security solutions essential.
4. **Data Privacy and Integrity**: IoT devices generate a vast amount of data, which often includes sensitive personal or business information. Ensuring the privacy and integrity of this data is critical, particularly in compliance-driven sectors like healthcare and finance.
5. **Physical Security**: The physical nature of IoT devices makes them vulnerable to direct tampering, which can compromise the entire network.

To conceptualize the challenge, consider the IoT Security Complexity Equation:

$$\textbf{Complexity} = (\text{Number of Devices}) \times (\text{Diversity of Protocols}) \times (\text{Security Requirements}) \quad (1)$$

This equation demonstrates how the complexity of security management in IoT networks increases with the number of devices, diversity of protocols, and the depth of security requirements.

Example: IoT Network in a Smart City

For instance, in a smart city scenario involving 10,000 IoT devices that utilize 5 major communication protocols (e.g., MQTT, CoAP, HTTP, LwM2M, Zigbee) and have 3 distinct levels of security requirements ((basic encryption, multi-factor authentication, continuous integrity checks), the complexity can be calculated as follows:

$$\textbf{\textit{Complexity}} = 10{,}000 \times 5 \times 3 = 150{,}000 \quad (2)$$

This complexity score of 150,000 indicates a high level of security management difficulty due to the large number of devices, the variety of protocols, and the layered security requirements. Each factor in the equation significantly impacts the overall security complexity:

- **Scalability:** A large number of devices (10,000) increases the potential points of failure and entry for cyber-attacks. Managing security configurations and updates for thousands of devices requires automated systems and rigorous protocols.
- **Diversity of Protocols (5):** Multiple communication protocols mean that security measures must be compatible across all protocols. It is noticed that TE and TM modes play a significant role in engineering secure communication channels within IoT systems by enhancing signal control, reducing interference, and minimizing vulnerabilities to external threats [11]. Each protocol may have different vulnerabilities and require different security approaches, which complicates the security management process.
- **Security Requirements (3):** Multiple layers of security controls, from basic encryption to more sophisticated measures like continuous integrity checks and multi-factor authentication, need to be implemented and maintained. This increases the complexity as each device must meet all these layered requirements to ensure network integrity.

This practical application of the IoT Security Complexity Equation in a smart city context illustrates the multifaceted nature of IoT security management. It highlights the necessity for strategic planning and the implementation of scalable, protocol-specific, and multi-layered security solutions to address the unique challenges of IoT environments.

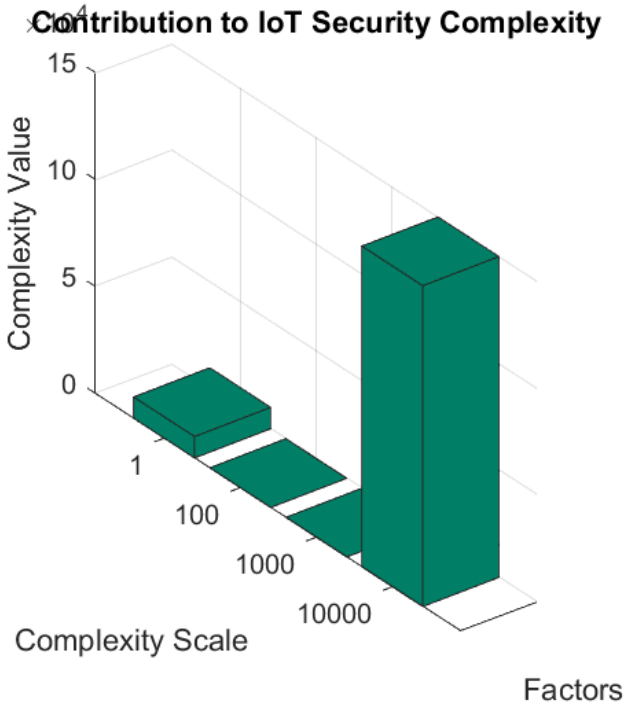

Figure 1: 3D Representation of IoT Security Complexity Contributions

This graph as depicted in Figure 1 highlights the individual impacts of the number of devices, diversity of protocols, and security levels on IoT security complexity, as well as their cumulative effect when combined. The stark contrast between the first three bars and the much taller final bar visually underscores the exponential increase in complexity when all factors interact. This demonstrates the multiplicative nature of security challenges in IoT environments, emphasizing the need for scalable and robust security solutions that address multiple factors simultaneously.

B. The Role of Authentication and Access Control

Authentication and access control are foundational elements in securing IoT systems. They address the identified challenges in the following ways:

1. **Authentication**:
    - **Purpose**: Authentication verifies the identity of devices and users, ensuring that only authorized entities can access the network.
    - **Methods**: This includes everything from simple password-based methods to advanced biometrics and cryptographic keys.
    - **Impact**: Effective authentication reduces the risk of unauthorized access and limits potential points of entry for attackers.
2. **Access Control**:
    - **Purpose**: Once an entity is authenticated, access control mechanisms determine the resources and actions that are permissible for that entity.
    - **Models**: Common models include Role-Based Access Control (RBAC), which assigns permissions based on pre-defined roles, and Attribute-Based Access Control (ABAC), which uses policies that evaluate attributes (characteristics) of entities.
    - **Impact**: Proper access control ensures that even if entities are compromised, the damage they can do is contained.

The effectiveness of these mechanisms can be visualized through a comparative table of access control models, illustrating their suitability for different IoT scenarios:

Table 1: Comparison between different access control models:

Model	Flexibility	Complexity	Best Use Case
RBAC	Low	Medium	Environments with stable, defined roles
ABAC	High	High	Dynamic environments requiring flexible access control
Policy-Based	Medium	High	Scenarios needing detailed, nuanced control settings

This table highlights the need to tailor access control strategies to the specific requirements and challenges of the IoT environment.

Overall, understanding the multifaceted security challenges of IoT and implementing effective authentication and access control systems are vital for safeguarding these interconnected networks. By addressing these aspects thoroughly, stakeholders can significantly enhance the security posture of their IoT ecosystems.

III. Exploring Authentication in IoT

Authentication in the Internet of Things (IoT) is a critical security measure to verify the identity of devices and users, ensuring that only authorized entities can access the network and perform actions. This section explores various

authentication mechanisms suitable for IoT systems, highlights the challenges these systems face, and discusses potential solutions to enhance security.

A. Overview of Authentication Mechanisms

Authentication mechanisms in IoT can be categorized based on the technologies and methods they employ. Here are some common approaches:

1. **Traditional Password-Based Authentication**: Simple but increasingly vulnerable due to the ease of password cracking and the difficulty of managing secure passwords across numerous devices.
2. **Digital Certificates and Public Key Infrastructure (PKI)**: Utilizes cryptographic keys for secure device authentication, offering higher security than traditional methods but at increased computational and management cost.
3. **Biometric Authentication**: Employs biological characteristics such as fingerprints or retinal scans. While highly secure, it's generally used more in user-centric scenarios due to hardware requirements.
4. **Token-Based Authentication**: Uses security tokens that devices present when making requests, suitable for scenarios where continuous connectivity might not be available.
5. **Behavioral Authentication**: Analyzes the typical behavior patterns of users or devices, using deviations from these patterns to flag potentially unauthorized access.

Each method has its own strengths and weaknesses, often tailored to specific types of IoT applications as mentioned in the following table:

Table2: Comparison of Authentication Mechanisms in IoT

Authentication Method	Strengths	Weaknesses	Typical Use Cases
Password-Based	Simple and familiar; Low cost	Vulnerable to attacks; Scalability issues	Consumer IoT devices, like smart home appliances
Digital Certificates (PKI)	High security; Scalable across large networks	Higher cost; Complex management	Industrial IoT, Healthcare IoT devices
Biometric Authentication	Highly secure; Difficult to forge	High implementation cost; Privacy concerns	High-security areas, like smart locks in smart homes
Token-Based Authentication	Doesn't require continuous connectivity; Scalable	Potential for token theft; Token management	Smart city applications, remote IoT devices
Behavioral Authentication	Dynamic security measure; Hard to replicate	Can require extensive data collection; Privacy issues	User-centric IoT devices, personal devices

- **Password-Based Authentication**: While easy to implement and familiar to most users, passwords are increasingly seen as less secure due to the prevalence of password cracking tools and techniques, making them suitable mostly for less critical applications.
- **Digital Certificates (PKI)**: Utilizing cryptographic keys within a Public Key Infrastructure offers robust security and is effective for managing authentication across vast networks with many devices, making it ideal for sectors where security is paramount.
- **Biometric Authentication**: This method leverages unique physical characteristics of individuals, offering high security but often at a higher cost and with potential privacy implications, thus its use is typically reserved for environments where security needs justify the expense and privacy trade-offs.

- **Token-Based Authentication**: Useful in scenarios where devices may not maintain constant network connectivity, token-based authentication provides a flexible and scalable option but requires careful management of the security tokens themselves to prevent loss or theft.
- **Behavioral Authentication**: By analyzing user behavior patterns, this method offers a dynamic and potentially more secure form of authentication. However, it relies on collecting and analyzing significant amounts of data, which can raise privacy concerns.

  Table2 not only presents a quick reference for comparing the effectiveness and applicability of different authentication methods in IoT but also aids in understanding the strategic trade-offs between security, cost, complexity, and user experience.

B. Challenges and Solutions for IoT Systems

Challenges:

1. **Scalability**: Managing authentication in a network with potentially millions of devices poses logistical and computational challenges.
2. **Resource Constraints**: Many IoT devices have limited processing power and storage, restricting the use of sophisticated authentication methods.
3. **Interoperability**: IoT devices often come from different manufacturers and may use incompatible authentication protocols.
4. **Security vs. Usability**: Balancing strong security measures with user convenience remains a critical challenge, especially in consumer IoT products.

Solutions:

To address these challenges, a combination of strategies is often employed:

1. **Hybrid Authentication Models**: Combining multiple authentication methods to balance security with resource constraints. For instance, lightweight cryptographic methods can be used in conjunction with simpler token-based systems.
2. **Edge Computing**: Processing authentication requests at the edge of the network can reduce latency and decrease the load on central servers, enhancing scalability.
3. **Standardization of Protocols**: Developing and adopting industry-wide standards can improve interoperability among devices from different manufacturers.
4. **Machine Learning**: Employing machine learning algorithms to enhance behavioral authentication methods, making them more effective and adaptable to new threats.

To illustrate the effectiveness of combining these solutions, consider the following equation for the **Probability of Authentication Success (PAS)**:

$$PAS = 1 - \prod_{i=1}^{n}(1 - p_i) \tag{3}$$

Where p_i is the success rate of the *i-th* authentication mechanism, and n is the number of mechanisms involved. This equation shows that using multiple, overlapping authentication methods can significantly increase the overall reliability of the system.

Combining different authentication methods improves the overall success rate. Indeed, the figure (Figure2) presents the success rates of individual authentication methods and their combined effectiveness, clearly illustrating the benefit of a hybrid approach to authentication in IoT systems. Three specific authentication methods typically used in IoT systems: PKI (Public Key Infrastructure), Token-Based, and Behavioral Authentication.

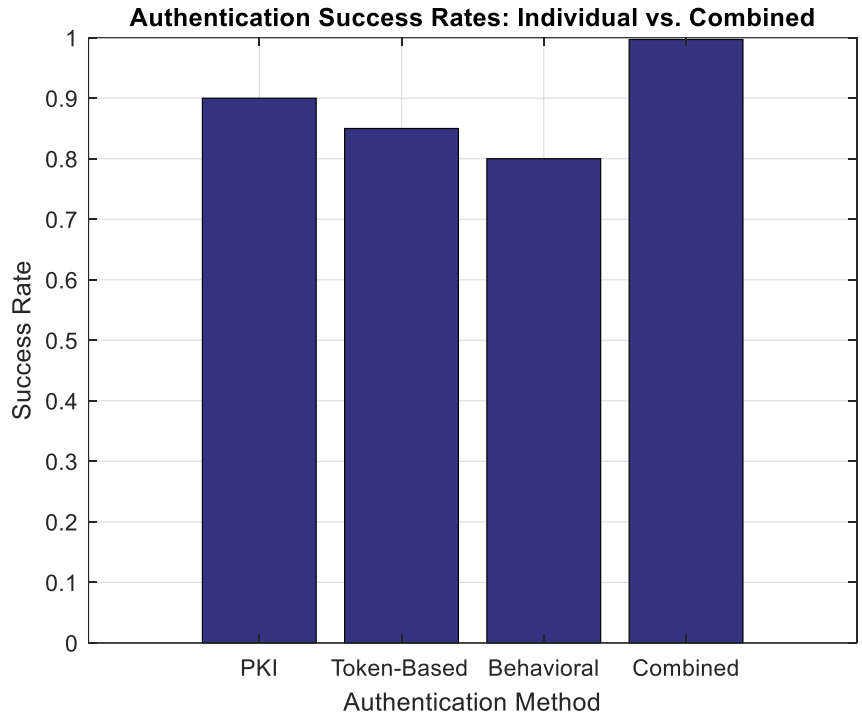

Figure2: Authentication Success Rate Improvement

This graph effectively illustrates the enhanced reliability of IoT authentication when multiple mechanisms are employed together. The individual success rates for PKI, Token-Based, and Behavioral Authentication are high, yet the combined success rate surpasses each individual method, visually underscoring the principle that layering multiple security measures significantly boosts the overall security posture. This graph supports the argument for hybrid authentication models in IoT systems, demonstrating that integrating various methods can effectively mitigate potential vulnerabilities and enhance system resilience against unauthorized access.

IV. Access Control in IoT Environments

Access control is a fundamental aspect of security in Internet of Things (IoT) systems, ensuring that only authorized users and devices can access certain data or perform specific actions. This section explores the various types of access control models and outlines best practices for implementing effective access control in IoT environments.

A. Types of Access Control Models

Access control models are essential for managing permissions within IoT systems, ensuring that only authorized users and devices can access sensitive data or perform specific actions. Below are the most common models used in IoT:

1. **Discretionary Access Control (DAC):** This model allows the resource owner to decide who can access it. While DAC offers high flexibility, it is generally less secure in IoT environments due to the potential for permission mishandling or accidental exposure of resources.
2. **Mandatory Access Control (MAC):** MAC enforces access policies determined by a central authority, ensuring a high level of security. However, it is less flexible and can be cumbersome to manage in dynamic IoT systems. It is most suitable for environments where strict security protocols are necessary, such as in military or government applications.
3. **Role-Based Access Control (RBAC):** RBAC assigns permissions based on predefined roles within an organization. This approach simplifies management and ensures consistency in access permissions. However, it may limit flexibility in dynamic or rapidly changing IoT environments, where roles may not always align with real-time needs.

4. **Attribute-Based Access Control (ABAC):** ABAC uses policies that evaluate various attributes (such as user identity, device type, location, and time) to grant access. This model offers high flexibility and fine-grained control, making it ideal for heterogeneous IoT environments with diverse and evolving access requirements.
5. **Policy-Based Access Control (PBAC):** PBAC builds on the ABAC model by emphasizing the use of external policies that can dynamically adjust permissions based on real-time data and changing conditions. This model provides high flexibility and security, making it suitable for complex and adaptive IoT systems where access needs to be continuously updated based on contextual information.

Each of these models addresses different requirements and risks associated with IoT security. The choice of model depends on the specific needs of the IoT system, including the level of security required, the complexity of the environment, and the need for flexibility in managing access.

In the following comparison, we evaluate these access control models based on four key factors: flexibility, security level, complexity of management, and best-suited environments. Table 3 illustrates this comparison.

Table3: Comparison of Access Control Models

Model	Flexibility	Security Level	Complexity of Management	Best Suited For
DAC	High	Low	Low	Small networks with trusted users
MAC	Low	High	High	High-security environments like military
RBAC	Medium	Medium	Medium	Organizations with clear role hierarchies
ABAC	High	High	High	Dynamic environments with complex access needs
PBAC	High	High	Very High	Environments needing adaptive policies based on real-time data

Impact of Access Control Type

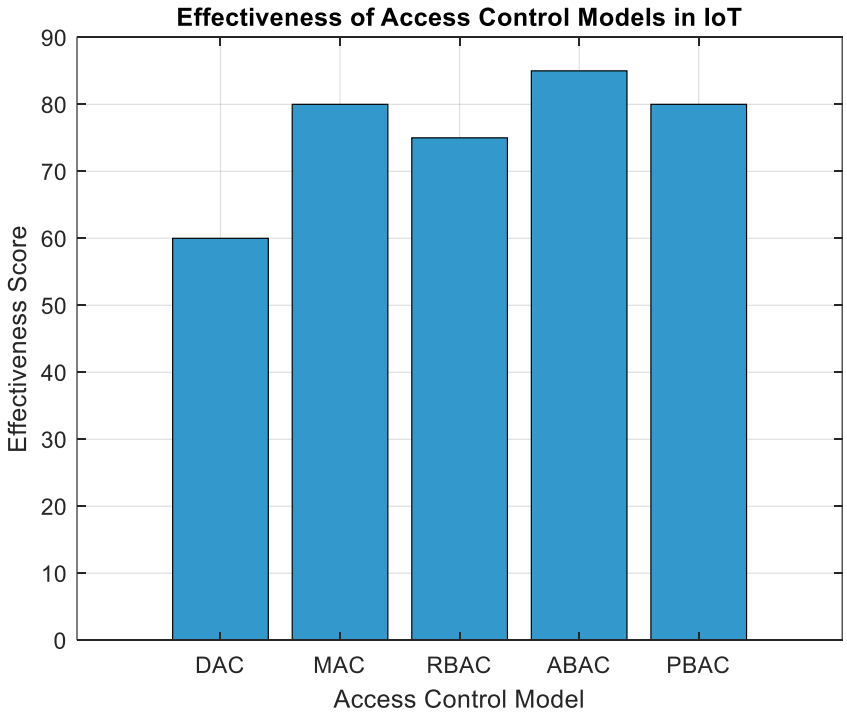

Figure 3: Effectiveness of Access Control Models in IoT

The bar graph as depicted in Figure 3 compares the hypothetical effectiveness scores of different access control models used in IoT environments, highlighting the suitability of each model based on its security features and flexibility. It shows that ABAC and PBAC are generally more effective in IoT contexts, given their higher scores. This is due to their ability to provide dynamic and fine-grained access control, which is crucial in managing the diverse and distributed nature of IoT devices. Conversely, DAC, while flexible, scores lower due to its security vulnerabilities in complex IoT environments. This visualization aids in understanding the strategic application of different access control models depending on specific security requirements and operational contexts in IoT systems.

B. Best Practices for IoT Security through Access Control

To enhance the security of IoT systems through effective access control, several best practices are recommended:

1. **Least Privilege Principle**: Ensure that users and devices have only the minimum level of access necessary to perform their functions. This limits potential damage in case of a security breach.
2. **Regular Updates and Reviews**: Continuously update and review access control policies to adapt to new threats and changes in the network or user roles.
3. **Use of Secure and Dynamic Policies**: Implement policies that are not only secure but also adaptable to changes in the context, such as user location or device status.
4. **Integration with Authentication**: Combine access control with robust authentication mechanisms to enhance overall security.
5. **Employment of Encryption**: Use encryption to protect control policies and the data they govern, especially when transmitted over networks.

Complexity of Access Control Management

The complexity of managing access control in IoT can be modeled by considering the number of devices, the number of access rules per device, and the interaction complexity between different devices and rules. The equation is given as:

$$\textit{Access Control Complexity} = (\textit{Number of Devices}) \times (\textit{Rules per Device}) \times (\textit{Interaction Complexity}) \quad (4)$$

Where:

- **Number of Devices** represents the total number of IoT devices in the system.
- **Rules per Device** denotes the average number of access control rules applied to each device.
- **Interaction Complexity** factors in the complexity arising from interactions between different devices (e.g., a multiplier based on device heterogeneity).

This equation helps to quantify how changes in the network scale, policy detail, and device interaction complexity impact the overall challenge of managing access control.

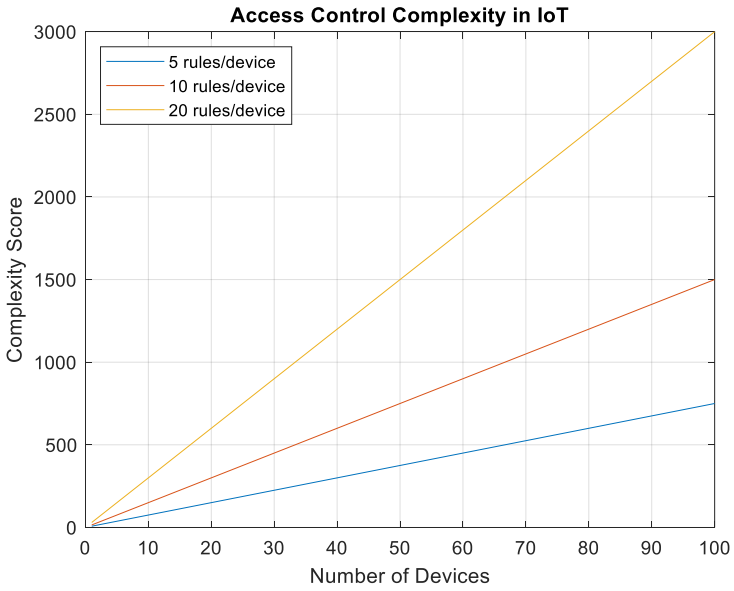

Figure 4: Complexity of Access Control in IoT

Figure 4 illustrates how the complexity of access control escalates with the increasing number of devices and the corresponding rules per device. As both the number of devices and the rules governing each device grow, the complexity of managing access control rises significantly. This visualization highlights the scalability challenges that IoT environments face, particularly as systems expand and become more diverse. It underscores the importance of considering these factors when designing and managing large-scale IoT systems.

V. Case Studies and Applications: Insights into IoT Security Implementations

Implementing robust IoT security strategies is crucial for protecting sensitive data and ensuring reliable device operation across various industries. This section delves into specific case studies that illustrate the implementation of IoT security measures and the lessons learned from these real-world applications.

A. Smart Home Security Implementation

Background: Smart home technology integrates various IoT devices such as thermostats, lighting systems, and security cameras into a single network that enhances the home living experience. Security, however, is a major concern, as personal space and data are at stake.

Implementation: In a typical smart home setup, manufacturers implemented a combination of advanced authentication mechanisms and encryption protocols to secure device communication and user data [12]. Role-Based Access Control (RBAC) was widely adopted to ensure that only family members could control devices based on their assigned roles.

Lessons Learned:

- **Encryption is Essential**: Continuous updates and strong encryption were crucial in protecting communication between devices and cloud services.
- **User Access Must Be Strictly Controlled**: Implementing RBAC helped prevent unauthorized access but required careful configuration to ensure ease of use without compromising security.

B. Healthcare IoT for Remote Patient Monitoring

Background: IoT devices in healthcare, such as wearable health monitors and remote patient tracking systems, need stringent security to protect sensitive health data and ensure the accuracy and reliability of medical information.

Implementation: Healthcare applications used Attribute-Based Access Control (ABAC) to manage access based on dynamic attributes like location, time, and the type of data requested. Data was encrypted both in transit and at rest, with regular security audits to maintain compliance with health regulations like HIPAA.

Lessons Learned:

- **Compliance is Key**: Regulatory compliance was essential in designing IoT solutions to ensure privacy and security standards were met.
- **Adaptive Security Policies Are Necessary**: ABAC allowed for flexible and adaptive security policies that responded to contextual changes, enhancing data security without impeding medical professionals' access to critical information.

C. Industrial IoT (IIoT) for Manufacturing Efficiency

Background: In industrial settings, IoT devices are used to monitor and control manufacturing processes, track assets, and manage supply chains. The security of these systems is critical to avoid disruptions and protect against industrial espionage.

Implementation: Industrial IoT platforms often used a hybrid approach combining MAC for critical system components and RBAC for user access management. Networks were segmented to isolate critical devices and minimize the potential impact of a breach. Blockchain technology was introduced for secure, tamper-proof logging of data exchanges.

Lessons Learned:

- **Network Segmentation is Crucial**: Segregating the network helps contain breaches and minimize their impact on critical industrial processes.
- **Hybrid Access Control Models Offer Flexibility and Security**: Using different models for different needs within the same environment provided both security and operational flexibility.

D. Comparative Analysis of IoT Security Approaches

The effectiveness of various security strategies across key IoT sectors can be visualized by examining their impact on system reliability and data integrity. Figure 5 presents a bar graph comparing the effectiveness of these strategies in three critical sectors: smart home, healthcare, and industrial IoT. The graph highlights that healthcare IoT achieves the highest effectiveness score, a result of the stringent security and compliance measures implemented in this sector. In contrast, industrial and smart home environments also show strong security performance but require strategies tailored to their unique operational needs and risk profiles.

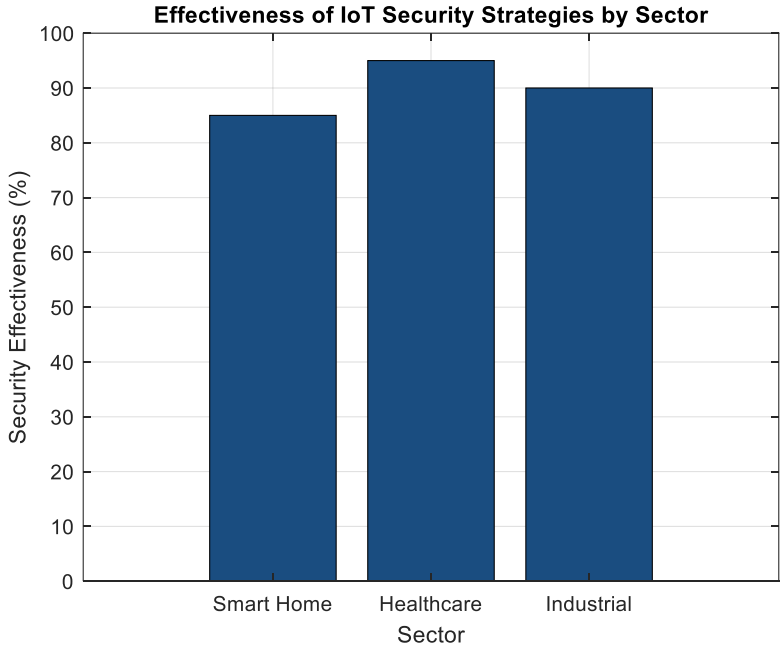

Figure 5: Effectiveness of IoT Security Strategies by Sector

These case studies offer valuable insights into the practical challenges and solutions in IoT security, demonstrating how diverse strategies are adapted to meet the specific requirements of different applications and environments.

VI. Conclusion

This paper has highlighted the pivotal roles of authentication and access control in enhancing the security of IoT networks. By exploring various authentication methods and access control models, we've underscored their effectiveness in addressing the unique security challenges posed by the IoT's scale and diversity. The insights from case studies in sectors like healthcare and smart homes demonstrate the practical impacts of these security measures. Moving forward, it's crucial that innovations in IoT security keep pace with technological advancements to safeguard sensitive data and ensure trust in IoT systems. Ultimately, the development of adaptable, robust security frameworks is essential for the sustainable growth of IoT ecosystems.

Acknowledgements

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2024-2443-03".

References

[1] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162-182.

[2] Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879*.

[3] Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A secure and decentralized authentication mechanism based on web 3.0 and ethereum blockchain technology. *Applied Sciences*, *13*(4), 2231.

[4] Abie, H., & Pirbhulal, S. (2024). Autonomous Adaptive Security Framework for 5G-Enabled IoT. *arXiv preprint arXiv:2406.03186*.

[5] Xu, H., Sun, Z., Cao, Y., & Bilal, H. (2023). A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. *Soft Computing*, *27*(19), 14469-14481.

[6] Pal, S., Dorri, A., & Jurdak, R. (2022). Blockchain for IoT access control: Recent trends and future research directions. *Journal of Network and Computer Applications*, *203*, 103371.

[7] Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, *7*(12), 25-43.

[8] Coiduras-Sanagustín, A., Manchado-Pérez, E., & García-Hernández, C. (2024). Understanding perspectives on personal data privacy in Internet of Things (IoT): A Systematic Literature Review (SLR). *Heliyon*.

[9] Kabir, M. S., & Alam, M. N. (2023). IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review. *International Research Journal of Engineering and Technology (IRJET)*, *10*(05), 1777-1789.

[10] Raeisi-Varzaneh, M., Dakkak, O., Alaidaros, H., & Avci, İ. (2024). Internet of Things: Security, Issues, Threats, and Assessment of Different Cryptographic Technologies. *Journal of Communications*, *19*(2).

[11] Klai, Z., Ayari, M., Hammami, M. A., Kefi, K., Gharbi, A., & Yahya, A. E. (2024). Electromagnetic Transverse Modes in Periodic Structures: Mathematical Analysis and Engineering Applications. *Journal of Electrical Systems*, *20*(7s), 713-726.

[12] Alkhonaini, M. A., Gemeay, E., Zeki Mahmood, F. M., Ayari, M., Alenizi, F. A., & Lee, S. (2024). A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata. *Scientific Reports*, *14*(1), 16701.