ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

Identity and Access Management for the Internet of Things (IoT)

Sampath Talluri

Department of Computer Science, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008

ABSTRACT

The ease with which intelligent gadgets may connect to the internet is a significant factor contributing to their rapid increase in popularity. The increasing popularity of smart gadgets is attributed to numerous factors, including their ability to introduce various unexplored opportunities in multiple industries. User ID administration should be more attention when developing Internet of Things platforms. Recently, behavior has shifted as more individuals are embracing technologies that enable devices to be recognized and connected to platforms associated with the Internet of Things. This method aims to facilitate the integration of more fundamental security designs during the development of applications for the Internet of Things. Consequently, identity and access management have been swiftly embraced in several IoT business sectors. Ensuring the continuous protection of user information is the sole viable solution, albeit an unfavorable one.

***Corresponding author**

Sampath Talluri, Department of Computer Science, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008.

Received: March 04, 2022; **Accepted:** March 14, 2022; **Published:** March 22, 2022

Keywords: IoT, Security, IAM, Scalability

Introduction

Background

Several IoT gadgets already come with inherent password protection. Customers are explicitly advised to replace them after making a purchase. Nevertheless, individuals vary in their level of meticulousness when it comes to monitoring information and responding appropriately. In addition, individuals who often change their passwords sometimes utilize credentials that are already publicly available. The limited processing capabilities of Internet of Things devices hinder the implementation of comprehensive security measures. This poses a challenge in implementing security measures, a primary concern in safeguarding these devices. Hence, it is imperative to deliberate about the suitable security measures for each device and devise a means to implement them without impeding the gadget's performance. This is quite inefficient regarding the device's connectivity to the Internet of Things [1].

The California Consumer Privacy Act (CCPA), implemented by the California state government, mandates that all networked Internet of Things applications must encrypt distinct passwords before being sold. However, there is a drawback. Several IoT devices with enhanced connectivity are connected to virtual personal assistants like Alexa and Siri. The audience must focus attentively during the presentation and make written records.

While numerous firms gather data using virtual assistants, not all information is fully comprehended. If all employees are aware of the passport, even those with restricted access can utilize the gadget. Alternatively, incorporating plugins and procedures is a feasible alternative.

Aim, Objectives and Research Questions

Aim

This study aims to assess how Identity and Access Management (IAM) contributes to the safety of IoT infrastructure.

Objectives

- To pinpoint particular difficulties associated with interoperability among different protocols and devices that make up the Internet of Things (IoT).
- To determine if the foundational features of IAM apply to IoT security.
- To ascertain how these characteristics protect the Internet of Things from various vulnerabilities and dangers.
- To assess the shortcomings of conventional identity and access management systems when tested across various platforms and devices.

Research Questions

- Regarding installing the Internet of Things, what are the most critical considerations for enterprises implementing an effective identity and access management solution?
- Is there a method for companies to ensure that their Identity and Access Management (IAM) system is interoperable with various IoT devices and platforms?
- Regarding the Internet of Things (IoT), how can Identity and Access Management (IAM) help make networks and devices more secure?
- Is there a way to improve identity and access management (IAM) systems to better handle the unique demands of an IoT setting?
- ow effective are conventional identity and access management (IAM) systems when faced with massive IoT rollouts?

Research Rationale

Every device connected to the internet can compromise network security through several means. An intruder who successfully infiltrates a single Internet of Things device can potentially compromise the entire network and expose highly sensitive data stored on all interconnected devices [2]. Consequently, they should be capable of establishing a connection to the network without encountering any problems. The absence of standardized protocols poses a significant security threat inside the Internet of Things realm. Ensuring compatibility and interoperability is challenging due to the proliferation of multiple platforms, protocols, and devices. Consequently, vulnerabilities may be established. Ransomware and the unauthorized takeover of Internet of Things devices pose significant risks to smart homes, healthcare monitoring systems, and wearable technologies.

The concept of a secure dwelling or an intelligent automobile that only activates when a specific requirement is fulfilled is somewhat alarming. These two options make me hesitate. Either of these two options requires substantial exertion. Individuals and companies continuously research and implement new security measures to proactively mitigate known dangers, as they are always seeking solutions. A key factor contributing to the susceptibility of internet-connected devices to security breaches is the insufficiency of computing power necessary for implementing robust built-in protection mechanisms. The limited resources available for developing and testing safe firmware contribute to the widespread existence of vulnerabilities.

Significance of the Research

Malicious individuals have a valid reason to worry about accessing confidential data stored on Internet of Things devices. Examples of sensitive military information include troop deployments, strategic blueprints, bank account numbers, credit card details, and personal information such as names, addresses, and passwords. Implementing identity and access management solutions can help save operational expenses. Federated identity systems have considerably eased application administration by removing the need to provide local IDs to external apps [3]. The swift progression of these technologies and their exorbitant expenses impose a burden on this budget. Ransomware encrypts data, renders equipment useless, and obstructs users from accessing related Internet of Things devices and platforms. Due to the rapid growth in the deployment of IoT devices worldwide, there needs to be more clarity surrounding this particular worry with IoT security.

Literature Review

Every identity and access management (IAM) system can manage contemporary authentication techniques. The inclusion encompasses biometric authentication, authentication without the need for passwords, authentication based on hardware (FIDO2), intelligent authentication, and various other ways. Every firm must effectively handle identities and other access forms following their information security policy.

This facilitates safeguarding sensitive data and information from constantly changing security risks. The organization can now efficiently identify policy violations and promptly revoke improper access privileges, eliminating the need to spend time and effort searching through different decentralized systems. The organization can perform these processes with the use of IAM solutions. Each solution offers a distinct method for actively identifying and addressing security vulnerabilities. To comply with audit and regulatory requirements, the organization may utilize identity and access management (IAM) to guarantee the implementation of appropriate security measures.

Company services are accessible to employees and end-users in a convenient manner, irrespective of the time or device used. This encompasses the ability to utilize company systems. IAM systems offer a range of contemporary authentication methods. Today, there is a wide range of authentication mechanisms accessible, including biometric, password-less, hardware-based, and smart options, among others. The password management functionality offered by Integrated Access Management (IAM) facilitates the implementation of password best practices. These recommended measures encompass robust authentication and regular password updates. Rest assured that Identity and Access Management (IAM) will accurately allocate the necessary privileges to the correct personnel in the proper locations [4]. On shared networks, there is a potential security risk associated with user credentials. The problem gets more complicated because employees have to handle credentials for many on-premises SaaS services and portals.

Frameworks for information access management (IAM) are necessary for role-based access control and restricting user access to critical information. System administrators can govern who has access to what within an organization's networks and systems by providing users with specialized rights. Positional power, duties, and job titles all define these positions [5]. Businesses can reduce operational costs in various ways, including selective access control and the ability to protect back-end technology such as APIs. Identity and Access Management (IAM) enables authorized users to securely access data from several sources, similar to a data pipeline.

The primary purpose of identity and access management systems is to validate individuals' or organizations' identities before providing access to apps and data. Users are typically authorized by logging in with a username and password. On the other hand, modern and future user authentication systems use artificial intelligence and other technical developments to better safeguard corporate assets.

Methodology

Data Collection

Secondary data is used in the paper because its low cost is the biggest advantage of adopting secondary data. Because someone else has already collected the data, the researcher saves time, energy, and money.

Because the data has already been collected, the researcher can save time, money, and energy during the data-gathering phase of their project.

Data Analysis

Thematic analysis is used in this paper because a flexible approach to data analysis can be used with the help of thematic evaluation. There are several advantages to using thematic analysis, which is why it is so popular and helpful for finding patterns in qualitative data. The flexibility of the thematic approach to qualitative research makes it a popular choice among researchers.

Tools and Techniques

Using resources like Google Scholar and the University Library will make it much easier for scholars to manage the vast amount of academic material and organize references.

Ethical Considerations

In studies of the built environment, both primary and secondary sources of information, or sometimes both, might be used. Secondary data research in the built environment is ethical since it saves time and resources, especially given the increasing difficulties in getting trustworthy primary data. Using secondary data is morally sound since it raises the ROI for any (public) data collection activities, simplifies research for respondents, assures that study results can be duplicated, and, ultimately, makes research procedures more transparent and honest.

Findings and Analysis

To adequately defend the Internet of Things (IoT) project, they should implement comprehensive permission control at every IoT platform's security level. If the IT defenses have any flaws, this will allow users to control them all. Before the Internet of Things, patients and doctors could only communicate through face-to-face meetings, phone talks, and written communication. There needed to be a rigorous strategy for healthcare institutions to consistently assess patients' well-being and provide guidance based on those assessments. The Internet of Things has developed as a technology that has the potential to dramatically benefit a wide range of enterprises across all industries. Installing IoT endpoint protection is one of the most critical things organizations can do to ensure the security of their Internet of Things devices. Endpoint security requires fixing vulnerabilities in essential ports such as UDP and TCP, securing wireless connections, and encrypting communications. It is critical to keep devices from becoming infected with dangerous software.

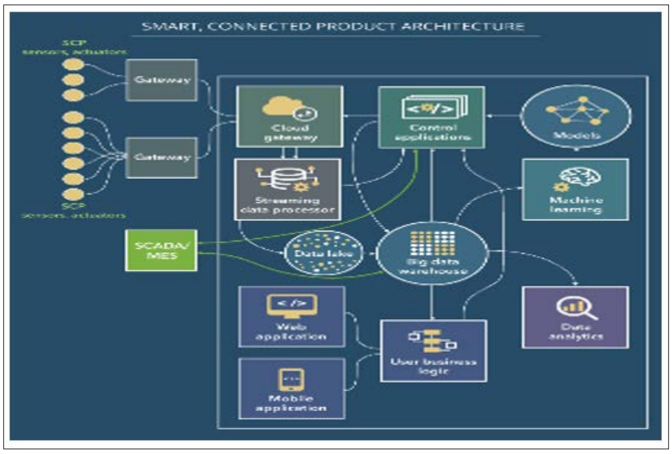

Figure 1: Elements of an IoT Architecture for Smart, Connected Products

This network of intelligent endpoints' ability to apply advances in numerous areas provides a more extensive and comprehensive service linked to healthcare, commerce, energy, information, and more. Internet of Things (IoT) devices capture data and send it to another network via the cloud. By safeguarding their endpoints, businesses may protect their networks from advanced threats like ransomware and malware. Furthermore, it protects devices at the network's periphery, allowing security professionals to view the whole picture, learn everything about the devices connected to it promptly, and reduce their vulnerability to threats. These devices encompass various hardware and software features, from typical home appliances and electronics to mobile phones and heavy industrial devices. Some IoT startups need to prioritize security to bring devices to market. It is likely that the device's security concerns were overlooked during development and that insufficient security upgrades will be available after distribution. Nonetheless, device security has improved with increased awareness of IoT security.

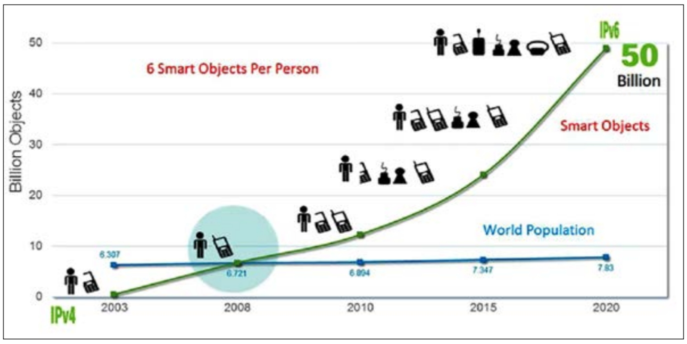

Figure 2: IoT Growth by Years

As a result of the growing acceptance of IoT technology models in many industries, such as manufacturing, healthcare, and automotive, a rising number of IoT devices are being used. Insurance companies can use IoT devices to validate claims by collecting sensor data. Changing the Way People Think About Health Internet of Things (IoT) solutions designed specifically for healthcare are becoming more readily available, which is positive. Furthermore, the huge amounts of data created by these linked devices can potentially transform the healthcare business.

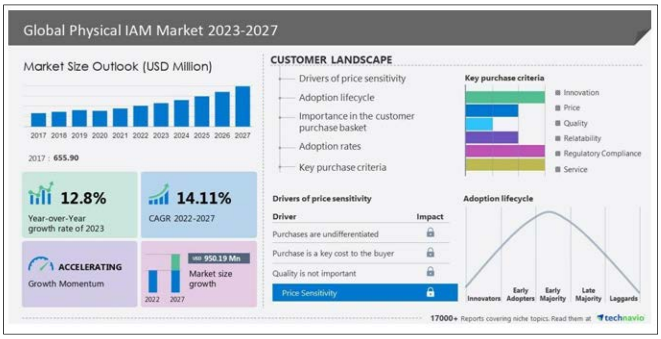

Figure 3: Global Physical IAM Market Potential

The value of the first phase can be used in the second, third, and fourth stages to gather and process even more data, respectively. Incorporating core values into the process makes it more intuitive and reveals attractive new business opportunities.

Implementing comprehensive security measures is a huge difficulty in safeguarding Internet of Things (IoT) devices due to their limited processing capabilities.

Conclusion

While the Internet of Things (IoT) has the potential to benefit businesses significantly, it may also entail significant organizational changes and present new risks. According to the first phase is configuring networked devices such as sensors, actuators, monitors, detectors, and video systems. These devices are in charge of gathering data. It is also typical for sensors and other devices to provide data in analog form. Before beginning data processing, it is necessary to collect and convert all of the data to digital form. Third, the consolidated and digitized data is transported to a data center or the cloud for additional processing and standardization. The fourth stage is to supervise and carefully examine the collected data. When this data is subjected to advanced analytics, it yields useful business insights.

Recommendation

A broad range of devices that can sense, communicate, and analyze data in various situations make up the Internet of Things (IoT), a conceptual framework. This area streamlines healthcare operations by outlining a fresh structure for interoperable systems and platforms that can communicate via the Internet protocol. Also, EcoStruxure allows communication with other widely used technologies through the Internet of Things (IoT), a complete framework for mobile health device data transmission. While several studies have looked at how the Internet of Things (IoT) may improve healthcare, how widespread its use will be in the insurance industry still needs to be discovered. As a result, a proper regulatory body to oversee and control the manufacturing of sensors must be established.

Further research is required to further the development of biodegradable material sensors. The ongoing development and modernization of technology have increased the importance of the Internet of Things (IoT) by necessitating the advantageous connecting of different electronic devices. In a nutshell, more efficiency in processes and operations is possible with IoT technology [6-9].

References

1. Partida A, Criado R, Romance M (2021) Identity and access management resilience against intentional risk for blockchain-based IOT platforms. Electronics 10: 378.
2. Zhu X, Badr Y (2018) Identity management systems for the Internet of Things: A survey towards blockchain solutions. Sensors 18: 4215.
3. Partida A, Criado R, Romance M (2021) Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms. Electronics 10: 378.
4. Carnley PR, Kettani H (2019) Identity and access management for the internet of things. International Journal of Future Computer and Communication 8: 129-133.
5. Yuan B, Jia Y, Xing L, Zhao DF, Wang XF, et al. (2020) Shattered chain of trust: Understanding security risks in crosscloud iot access delegation https://www.usenix.org/conference/usenixsecurity20/presentation/yuan.
6. Giaretta A, Pepe S, Dragoni N (2019) UniquID: A quest to reconcile identity access management and the IoT. In Software Technology: Methods and Tools: 51st International Conference, Innopolis, Russia 51: 237-251.
7. Grizhnevich A (2018) Evolutionary approach to an IoT architecture for smart, connected products. Science Soft https://www.scnsoft.com/blog/iot-architecture-for-smart-connected-products.
8. Nur M, Wang Y (2021) January. An overview of identity relationship management in the internet of things. In 2021 IEEE International Conference on Consumer Electronics (ICCE)
https://ieeexplore.ieee.org/document/9427723.
9. Aydos M, Vural Y, Tekerek A (2019) Assessing risk and threats with layered approach to Internet of Things Security. Sage Journal 52: 338-353.