THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 2 (2024)
https://doi.org/ 10.62019/abbdm.v4i02.178

Policy-Based Contextual Access Control Mechanism for Smart IoT Devices

Yasir Arfat Malkani, Poonam Bai, Lachhman Das Dhomeja, Muhammad Kamran Abbasi

Chronicle

Article history

Received: June 4, 2024
Received in the revised format: June 19, 2024
Accepted: June 20, 2024
Available online: June 22, 2024

Yasir Arfat Malkani & Poonam Bai, are currently affiliated with Institute of Mathematics & Computer Science, University of Sindh, Jamshoro, Pakistan.
Email yasir.malkani@usindh.edu.pk
Email:poonam.jessani@yahoo.com

Lachhman Das Dhomeja is currently affiliated with Department of Information Technology, University of Sindh, Jamshoro, Pakistan.
Email: lachhman@usindh.edu.pk

Muhammad Kamran Abbasi is currently affiliated with Department of Distance Continuing & Computer Education, University of Sindh, Jamshoro, Pakistan.
Email:abbasikamran@usindh.edu.pk

Corresponding Author*

Abstract

Access control remained an important aspect of computer security, and it has been the focus of extensive research over the past several decades. Access control mechanisms generally composed of two fundamental components: authentication and authorization. Authentication refers to verifying the identity of an entity, and authorization guarantees that only authenticated entity or devices can access the permitted devices or other resources. Various traditional access control schemes, such as Access Control Lists (ACLs), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) exist, but these have certain limitations that hinder their direct implementation in the Internet of Things (IoT). For instance, ACLs maintain user-specific access privilege lists, which are feasible for environments with limited users and devices, but impractical for large scale systems like IoT. RBAC assigns devices access through roles associated with permissions, however role management in dynamic IoT environments poses significant challenges. ABAC grants access based on user and devices attributes that requires certain attribute criteria for authorization. We advocate that IoT environments are dynamic in nature and consist of very large volumes of smart IoT devices (such as smart sensors, smart phones and gadgets) that which introduce unique access control challenges. One significant challenge is providing dynamic access to smart IoT devices, as opposed to relying on static rules, roles, or attributes. Considering these challenges, this research advocates for a novel access control scheme tailored for accessing smart IoT devices in internet of things environments. The prototype implementation of the proposed approach is carried out along with conducting the usability study to evaluate the performance and suitability of the proposed system for real world internet of things (IoT) scenarios.

Keywords: Security, Access Control Schemes, Context-Awareness, Smart IoT Devices, Access Policies.

INTRODUCTION

Kevin Ashton first presented the notion of internet of things (IoT) in 1999 (Ashton, 2017). Kevin envisioned an environment, where people and objects (such as devices, machines, or other real-world items) can interact anywhere and anytime (Kuyoro et al.,2015). Kevin proposed that, similar to the Internet, IoT has the potential to revolutionize human lifestyles globally. The IoT systems are composed of three (03) main components: the computing infrastructure, the physical objects themselves, and the communication network, which links these objects (Abdul-Qawy, et al., 2015; Rajpoot, et al., 2015). Currently, there exist numerous appealing and emerging IoT applications (Zhang & Liu, 2012; Zorzi et al., 2010; Ali et al., 2019) for monitoring, control, and automation. For instance, a smart home scenario features various smart devices that are connected to a main home controller through standardized Internet protocols (Godha et al., 2014; Kumar & Pati, 2016). These embedded smart home devices offer remote services to home owners and make it easy for them to achieve

their desired goals like turning lights on or off, adjusting light levels, controlling heating or air conditioning and managing window blinds. Another example of IoT scenario could be a healthcare system, where a nano-chip may be implanted in each registered patient to monitor his/her health in order to provide automatic assistance in critical or emergency situations (Remote Patient Monitoring Tools, 2017).

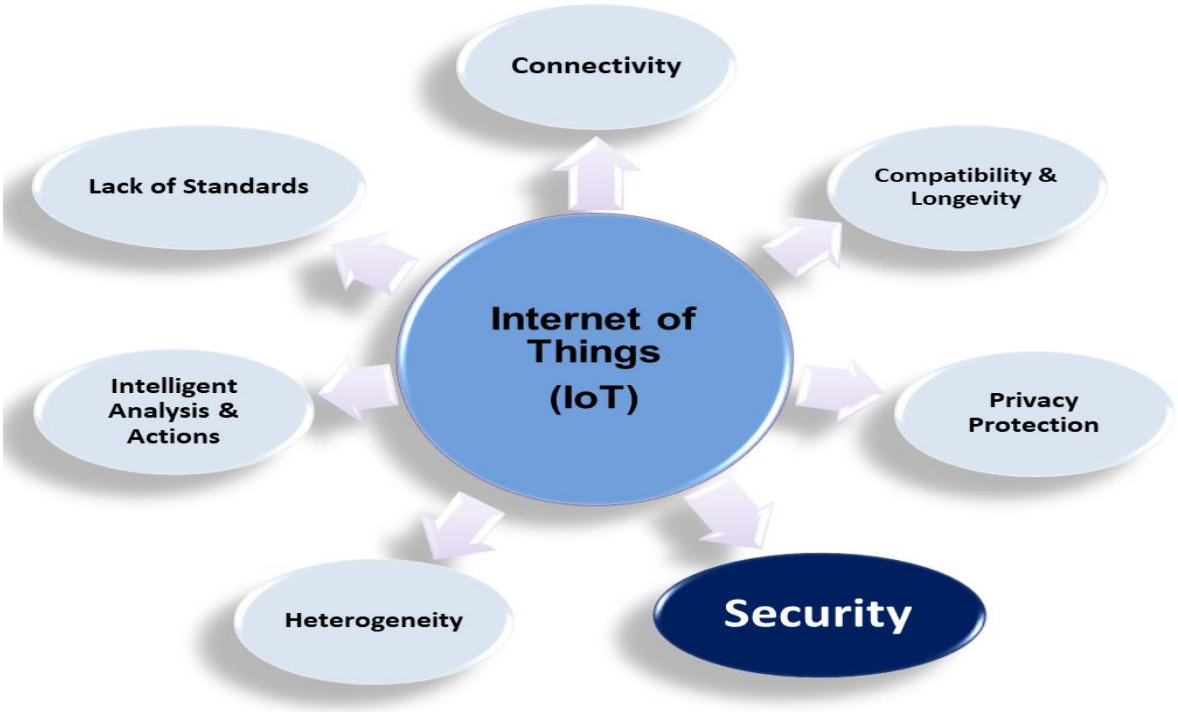


Figure 1.
The internet of things (IoT) research challenges

To fully realize IoT's potential, several research challenges (Banafa, 2017; Guillemin & Friess, 2009; Sicari et al., 2015; Gerber, 2019; Cerf, 2015; Salama et al., 2017; Ouaddah et al., 2016) must be addressed. Figure 1 shows the list of some of those research challenges, including security, heterogeneity, privacy protection, lack of standards, connectivity, and context-aware service provision, etc. This research specifically addresses the access control aspect of IoT security. Access control mechanisms restrict user access to resources based on their roles and privileges (Ouaddah et al., 2016). Although there is extensive literature on access control mechanisms, traditional methods cannot be directly applied to the IoT domain without modifications. Consequently, this research aims to propose and develop an access control mechanism for IoT environments particularly tailored to access smart IoT devices. The contributions of this work include: proposing an effective and efficient framework for access control in the IoT, prototype implementation and testing of the proposed approach, and a usability study to evaluate the proposed system's performance and suitability for IoT environments. This paper is organized into six (06) sections. The Introduction section outlines the research domain, overall work, and contributions. The Background section covers fundamental concepts and surveys access control mechanisms. In proposed approach section, the technical details of the proposed access control scheme are described. Implementation and testing details are given in system implementation section followed by results and discussion section, which presents findings from the usability study, highlighting the system's evaluation in real-world scenarios. Finally, the conclusion section summarizes the research, discusses

limitations, and suggests future directions.

BACKGROUND

Basic Concepts

Inter of Things (IoT): As previously mentioned, Kevin Ashton introduced the concept of the Internet of Things (IoT), envisioning a world where people and devices interact seamlessly anytime, anywhere (Ashton, 2019; Kuyoro et al., 2015). Internet of things architecture is consisting of three (03) layers: perception layer, the edge layer and the cloud layer (Abdul-Qawy et al., 2015; Rajpoot, Jensen, & Krishnan, 2015). The perception layer comprises a diverse array of IoT devices that interact with the physical world to gather data and information. The edge layer facilitates connectivity among IoT devices, managing their heterogeneity and providing essential services. The cloud layer is crucial for deploying components that handle tasks like collaborative interference detection and big-data analysis. Applications of IoT span various fields, including smart healthcare, smart cities, industrial environment monitoring, smart homes monitoring and control, vehicular networks monitoring and control, etc (Ali et al., 2019; Godha et al., 2014; Kumar & Pati, 2016).

Authentication and Authorization: Understanding authentication and authorization is vital for managing data and resource access. Authentication ensures that an entity is who it claims to be, while authorization determines an entity's credentials to access services based on its identity (Sicari et al., 2015).

Confidentiality: It makes sure that only authorized entities can access certain information or data. This is achieved through encryption, which prevents unauthorized users from decrypting or understanding the message text.

Access Control Mechanism: In figure 2, the scenario of an access control system is illustrated. It is a security feature that makes it possible to monitor and manage transparent access to both hardware and software system resources, and ensures that only authorized users can interact with system resources.

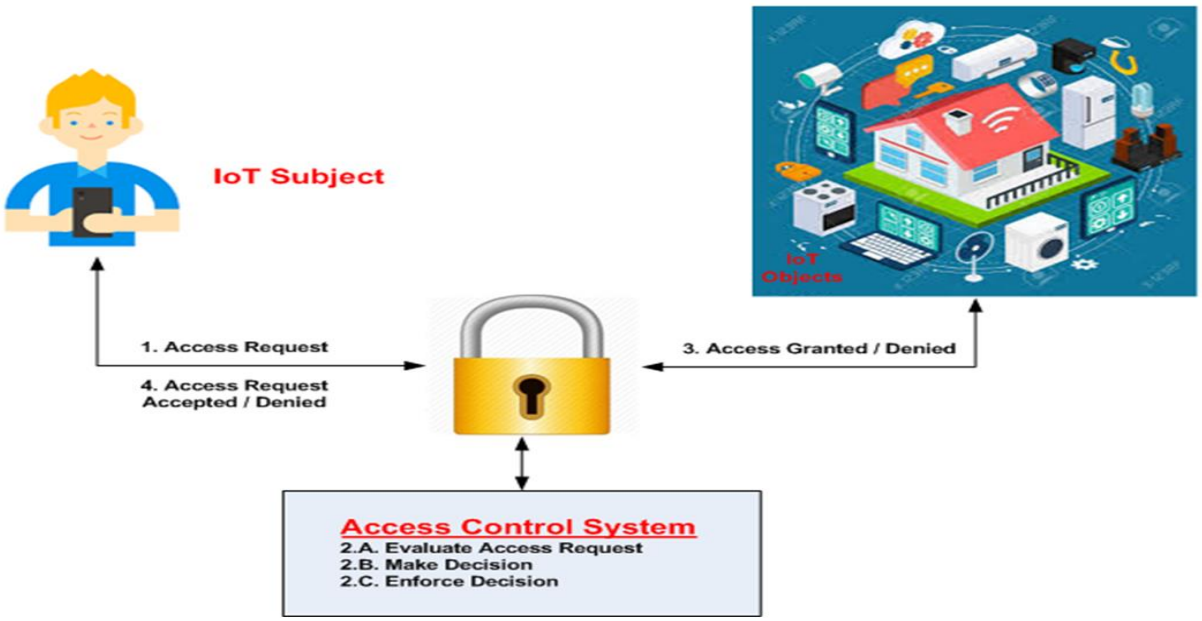


Figure 2.
An example scenario of access control in IoT

LITERATURE REVIEW

In Extensive work has been done on access control mechanisms and numerous approaches have been proposed by both industry and academia (Bertin et al., 2019; Zhang & Gong, 2011; Liu et al., 2017; Liu et al., 2012; Jindou et al., 2012; Zhang & Tian, 2010; Zhang & Liu, 2012; Zhang & Tian, 2010; Ouaddah et al., 2016; Gusmeroli et al., 2012; Mahalle et al., 2013; Mahalle et al., 2012; Barka et al., 2015; Jayant & Sulabha, 2014; Gerber, 2019; Guillemin & Friess, 2009) during last several decades. Amongst them, some prominent approaches to access control are discussed in this section. Let's begin the discussion with mandatory access control (MAC) approach (Jayant & Sulabha, 2014). The MAC approach permits only the owner for the management and to set preferences for the access control to smart IoT devices. In this approach, end-user has no authority and control over the settings that provide access privileges or rights to anyone. Next traditional access control mechanism is access control lists (ACLs). In contrast to MAC, ACLs provide a mechanism in which end-users or entities are given access to smart IoT devices or resources based on their roles (Bertin et al., 2019). Another conventional access control approach is the discretionary access control (DAC).

DAC allows a user to have complete control over the IoT resources they own, including any associated programs or applications (Jayant & Sulabha, 2014; Bertin et al., 2019). An important drawback of the DAC mechanism is that the permissions granted to the end-user are automatically inherited by any programs or applications they run, which means that if an end-user unknowingly runs a malicious program, like a malware, the malicious program could easily use the user's privileges to launch attacks on the resource or device owner (Jayant & Sulabha, 2014). In (Bertin et al., 2019) role-based access control (RBAC) approach is discussed and explained in detail. RBAC approach provides access to smart IoT devices and resources based on the role or designation of the user that she/he fills in an enterprise or institution. For instance, an HR section person may not be permitted to create user accounts to perform network related activities, because this is permitted role of a network or system administrator. Some other studies (Zhang & Tian, 2010; Barka, Mathew, & Atif, 2015; Bertin et al., 2019; Yuan & Tong, 2005) have also attempted to use the RBAC model for IoT system, however, these works (Zhang & Tian, 2010; Barka, Mathew, & Atif, 2015) do not adequately address the challenges faced by resource-constrained smart IoT devices, like smart sensors.

Next is the Capability-Based Access Control (CapBAC) approach that was basically conceived with the idea that IoT resources can issue keys, tickets, or tokens that later permit the holder to access certain entities or objects within an IoT system (Gusmeroli, Piccione, & Rotondi, 2012; Mahalle et al., 2013). Each smart IoT device, possessing a token, can grant or revoke access rights to another IoT device. An important drawback of this approach is that every device must generate tokens with specific capabilities, which is a quite challenging task in IoT environments. In addition to the conventional access control approaches mentioned above, some researchers have developed proprietary solutions. Notably, Zhang and Gong (2011) proposed a usage control (UCON) approach for IoT systems, which relies on fuzzy logic and centralized servers to manage IoT resource usage and access control decisions. Although, authors have provided a partial theoretical or qualitative evaluation, but this work lacks a comprehensive quantitative evaluation and does not address the practical feasibility of the proposed scheme (Zhang et al., 2011). Another research effort by Liu, Xiao and Chen (2012) presents an access control approach that combines Elliptic Curve

Cryptography (ECC) with the Role-Based Access Control (RBAC) model. ECC is exploited to establish secure keys, while RBAC is used to define policies for accessing IoT resources including smart IoT devices. This approach (Liu et al., 2012) is also incorporates OpenID technology (OpenID Home Page, 2024) and relies on trusted central security servers for authentication. since this approach uses RBAC, it inherits the limitations drawbacks associated with RBAC, as discussed previously. Mahalle et al. (2012) proposed an access control approach based on the capability-based access control model. Their work involves exchanging capabilities of IoT resources along with a SHA-1 message digest to ensure the integrity of the exchanged information. However, this study does not provide details on the content or representation of these capabilities, nor does it discuss the communication technologies used to implement the system. Additionally, the proposed scheme heavily depends on a central server for intensive computations related to Elliptic Curve Cryptography (ECC), which limits its applicability in decentralized IoT environments.

Context and Context-Awareness

In order to effectively and efficiently access smart IoT devices in internet of things landscape, it is essential to manage permissions based not only on user roles or attributes, but also by considering the dynamic nature of IoT. Contextual information plays an important role in determining access permissions as it provides specific details about the circumstances under which access requests are made. In IoT, context refers to any data (including location, time, identity, and the status of nearby by devices or networks) defining or characterizing the situation of an entity (Abowd et al., 1999). Figure 3 illustrates the classification of context. Context can be classified as computing, user, time, and physical context. Computing context encompasses factors such as device capabilities, network conditions, and computational resources available. User context involves user preferences, roles, and authentication status. Time context considers temporal aspects, including deadlines for tasks or the availability of resources at specific times. Physical context pertains to the environmental conditions surrounding IoT devices, such as temperature, humidity, and physical location (Soomro, 2019).

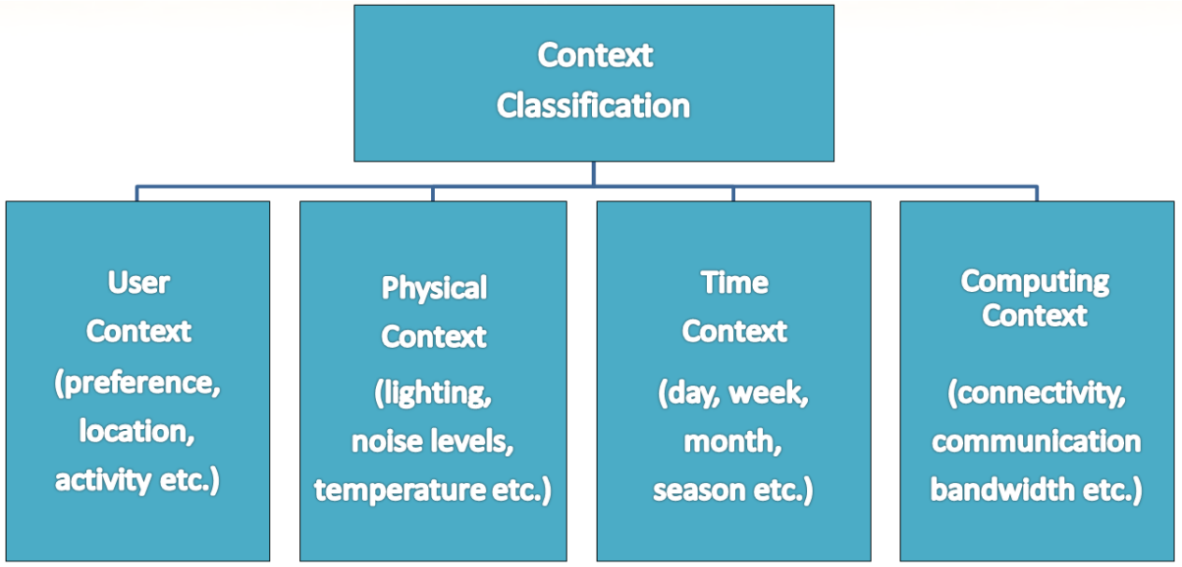


Figure 3.
Classification of context (Soomro, 2019)

Context-awareness goes beyond merely recognizing context. It involves utilizing context information dynamically to tailor services or responses accordingly. A context-aware system or application adjusts its behavior based on the context it perceives, enhancing user interactions and optimizing resource utilization in IoT environments (Abowd et al., 1999; Soomro, 2019). For instance, a smart healthcare system could adjust medication reminders based on a patient's location and health condition inferred from wearable devices. In summary, from the literature review, it becomes evident that while traditional access control models like MAC, DAC, RBAC, and CapBAC provide foundational approaches, they often overlook the dynamic and heterogeneous nature of IoT environments. Proprietary solutions, such as Usage Control (UCON) and capability-based schemes integrating cryptographic techniques, attempt to address these challenges but lack comprehensive evaluation or practical feasibility in real-world IoT deployments. Given these gaps, this research aims to develop a novel hybrid access control mechanism for IoT that integrates context and context-awareness with policy-based access control.

The Proposed Approach

The main objective of this research is to develop a robust access control mechanism specifically designed for IoT environments, ensuring secure management of access to IoT resources, including smart IoT devices, while integrating policies and context-awareness. Figure 4 shows the overall architecture of the proposed access control framework. Key components of the framework include IoT Subjects (IoTS) and IoT Objects (IoTO), IoT Secure Communication (SecCom) ensuring secure data transmission, Contextual Information (CI) component, which is crucial for informed access control decisions, and Access Control Management & Decision Logic (ACM&DL) component that is integrating access policies and IoT resources information to enforce policy based contextual access decisions.

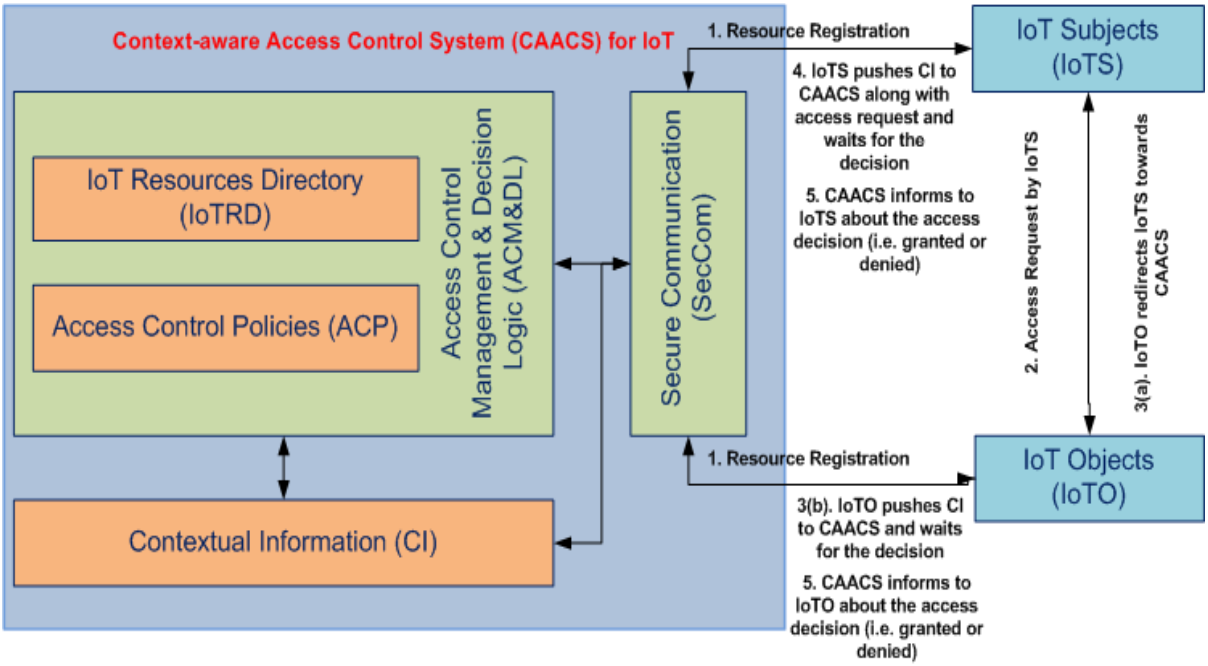


Figure 4.
High-level Architecture of the Proposed System

This structured framework ensures that our proposed access control mechanism effectively addresses the dynamic challenges posed by IoT environments, thereby

enhancing both security and operational efficiency in managing access to IoT resources. In this framework, IoT subjects act as clients initiating access requests, while IoT objects represent the resources that provide specific services. The first phase includes registration, where all IoT resources, whether subjects or objects, must register with the CAACS. While registering, the IoT resources provide their access control policies along with relevant device attributes that specify their computational and communication capabilities.

Once registration process is completed, then IoT subjects can request access to IoT objects. When an access request is initiated, the IoT object redirects the IoT subject to the CAACS and concurrently shares its contextual data with both the CAACS and the IoT subject. The CAACS checks and evaluates the access request by exploiting the access control policies and contextual data/information from both parties. Based on this evaluation, the CAACS reaches at the decision whether to deny or grant access, and then communicates this decision to the IoT subject and IoT object. A message sequence diagram is given in figure 5, which shows the major components and illustrates the overall working mechanism and flow of the proposed approach. Infact, this message sequence diagram provides a visual representation of how the system components interact, demonstrating how IoT resource access is managed securely and contextually.

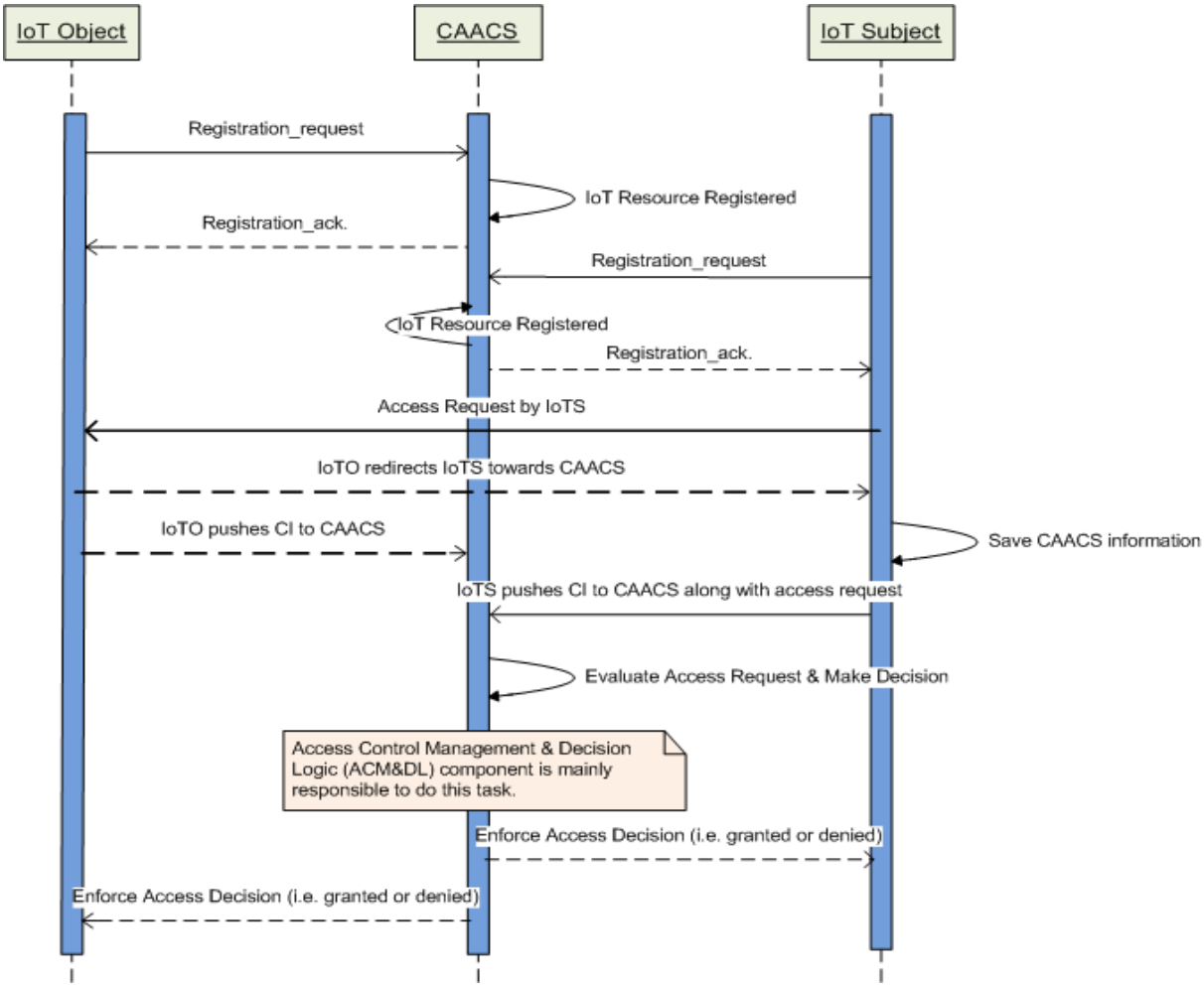


Figure 5.
Message Sequence Diagram (MSD) of the proposed approach

SYSTEM IMPLEMENTATION

This section provides a detailed account of the system implementation process for the proposed approach. The implementation of the proposed access control scheme leverages several tools and technologies to ensure robust functionality and practical viability:

- WiFi Hotspot Laptop: utilized as a connectivity hub for IoT devices interactions.
- Android Phones: devices equipped with the Android operating system, chosen for their widespread compatibility and open-source nature.
- Android Studio: employed as the primary Integrated Development Environment (IDE) for writing and debugging the prototype IoT application code (Android Studio Home Page, 2024). The development environment runs on a Core i7 computer with 16GB of RAM and a processing power of 3.2 GHz. Figure 6 showcases the Android Studio IDE.
- Operating System: The development setup operates on Windows 10 64-bit.
- ENCRYPT 5.0.5 library: used to maintain message confidentiality across various components of the system.

Apart from aforementioned tools, for the server-side implementation of the proposed system, Python 3.10.2 is selected, with Visual Studio Code 1.63.2 serving as the primary code editor. Additionally, modules such as PYCRYPTODOME 3.13.0, along with standard libraries like SOCKET, THREADING, and JSON, are imported to support comprehensive server-side functionalities.

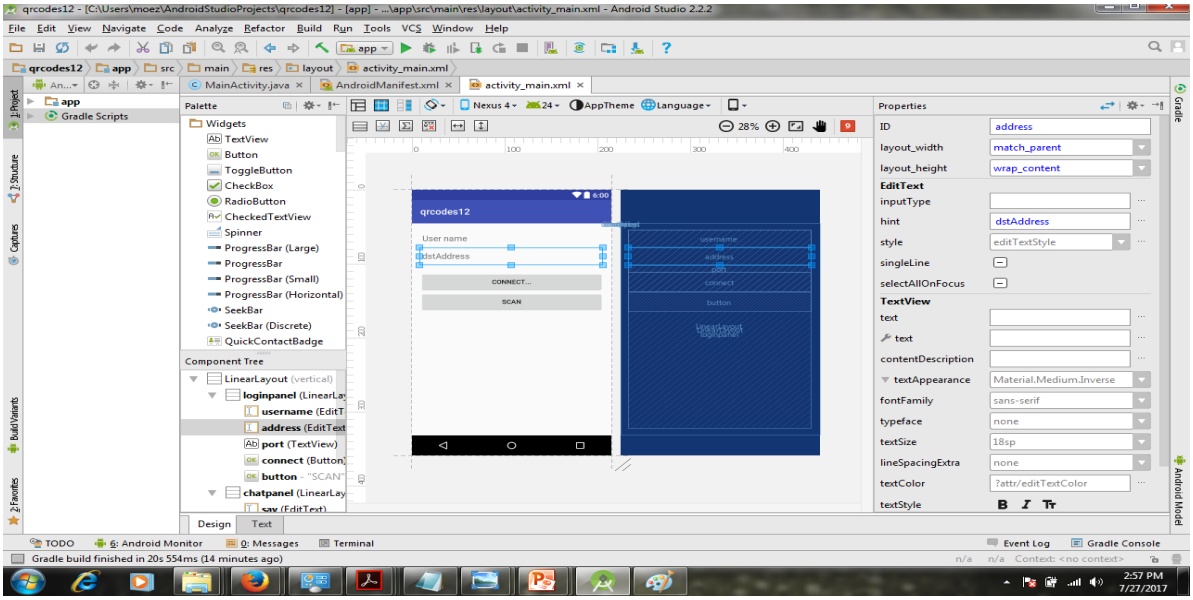


Figure 6.
Android Studio IDE (Android Studio Home Page, 2024)

To test the prototype system implementation, and to evaluate the proposed access control approach, a hypothetical healthcare scenario is developed and executed, which is described below: A patient named Imran is brought to the hospital's emergency room due to an unknown medical complication. Ahmed is the duty doctor at the hospital, who has to treat Imran in emergency situation, but he is not Imran's regular physician. For effective and proper treatment, Ahmed requires

immediate access to Imran's emergency medical records as well as data from his implanted/wearable healthcare smart IoT devices and sensors. Traditional access control approaches like role based access control (RBAC), access control lists (ACLs) or attribute based access control (ABAC) pose significant limitations in such dynamic internet of things scenarios. These existing approaches might restrict or prevent Ahmed from accessing Imran's medical information including data from his implanted sensors even in emergency or critical situations. We advocate that aforementioned scenario raises the dire need for contextual access control system, which is proposed and implemented in this work. The proposed system exploits contextual information and user-defined preferences and policies to grant Ahmed access to Imran's medical data during emergency or critical situations. This ensures that access decisions are made dynamically based on real-time context, enhancing the efficiency and effectiveness of healthcare delivery in critical/emergency situations.

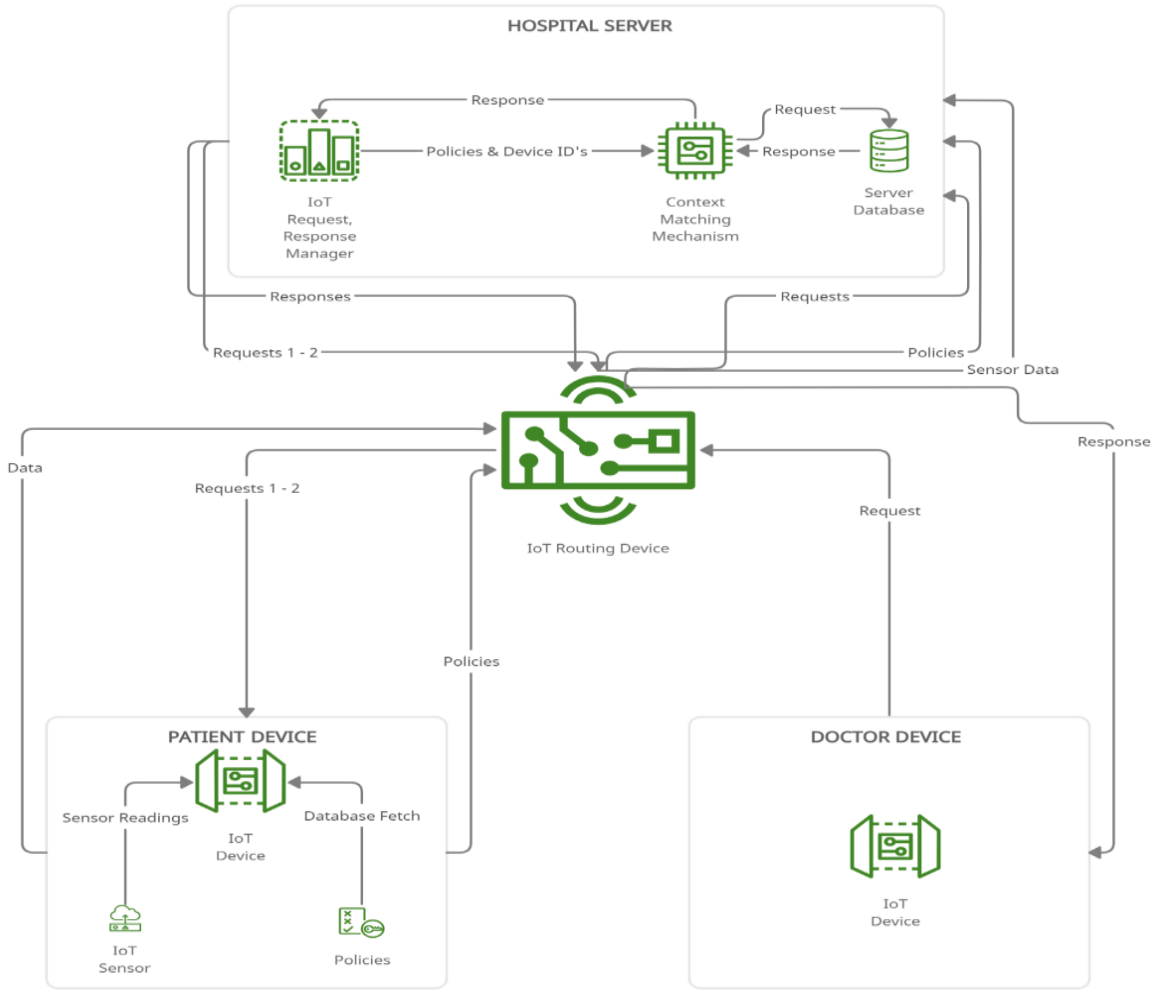


Figure 7.
Data Flow Diagram of Hypothetical Scenarios

The data flow diagram of the prototype implementation of the aforementioned hypothetical scenario is shown in figure 7. The three main components of the implemented scenario include: hospital server, doctor's IoT device, and patients IoT devices or implanted IoT sensors. Hospital server is the central component that stores and manages medical records of all registered patients, including individuals, such as Imran from the hypothetical scenario. It also maintains records of doctors and other

hospital staff. The hospital server stores global access policies and user-defined preferences. Next component is the doctor's IoT device that is used by doctors in order to facilitate them access to patient's medical records. It could be a handheld device, such as smart mobile phone or PDA, or a more sophisticated tool such as a PC or laptop. The third component is patient's smart IoT devices, which includes implanted sensors or other portable devices used by patients to record real-time medical data.

The depicted scenario in figure 7 indicates the practical application of the access control mechanism in managing sensitive medical data securely across IoT devices within a hospital environment. It serves as a pivotal illustration of how the proposed framework discussed earlier is translated into a functional system, validating its capability to address real-world challenges in IoT-based settings. Following the successful implementation of the system, rigorous testing is conducted in a controlled computer laboratory environment to validate its adherence to the proposed model. The testing phase involves thorough execution of various applications developed (as shown in figure 7) using the aforementioned tools and technologies. Description of each of the developed application is given below:

Patient Application: The Patient Application, designed for deployment on IoT devices used by patients, consists of three sub-components: (i) registration, (ii) sensor widgets, and (iii) policies. (i) Registration: Figure 8 illustrates the initial registration process of the patient application. This component collects patient names and server IP addresses, crucial due to potential dynamic changes in local IP addresses. Upon pressing the proceed button, user details are registered in shared preferences, a connection request is sent to the server, and the user is directed to the sensor widgets screen.

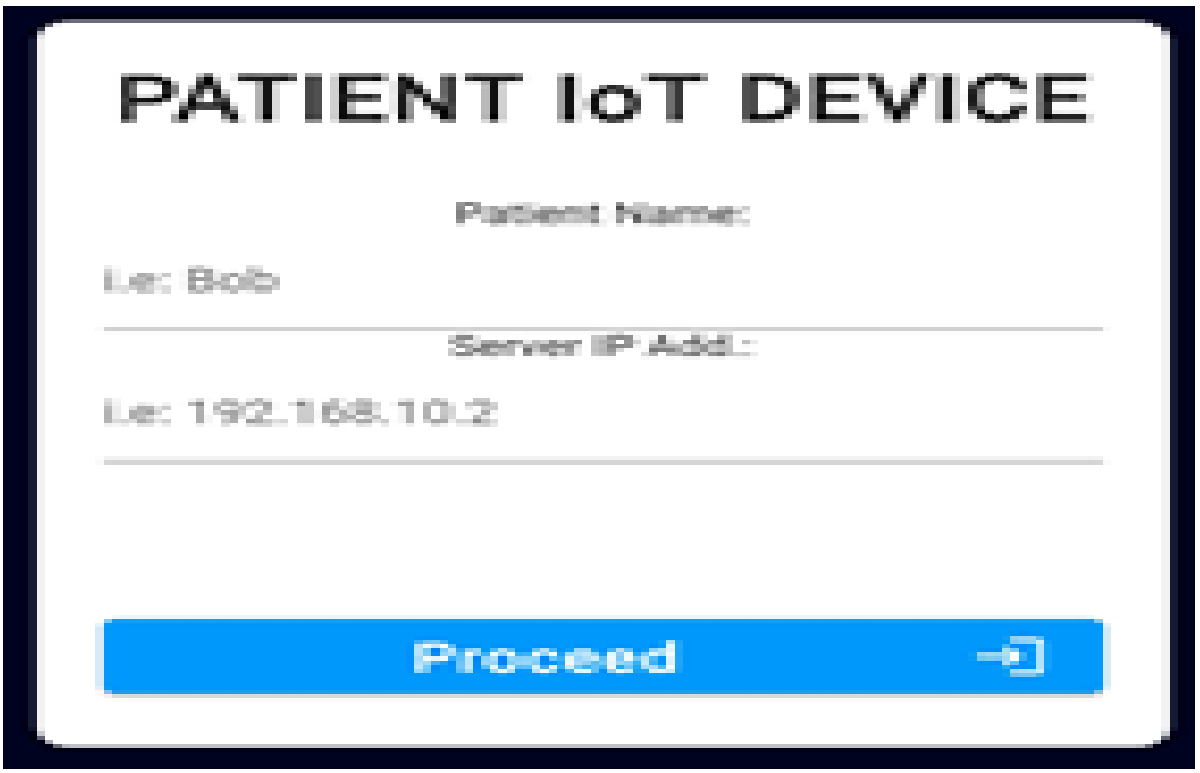


Figure 8.
Patient's application screenshot illustrating registration process

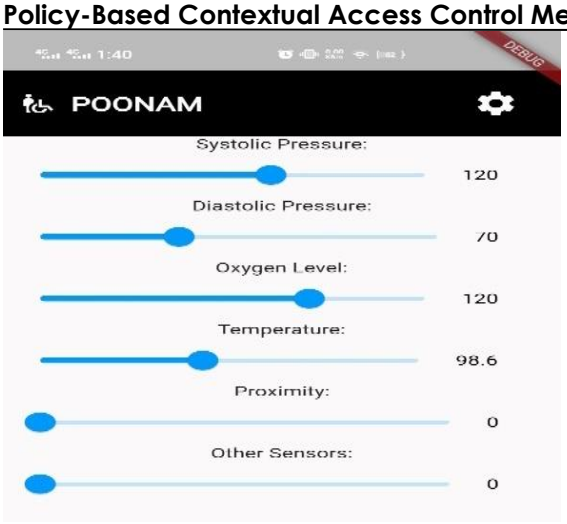


Figure 9.
(a): Sensor Widgets (Normal Condition)

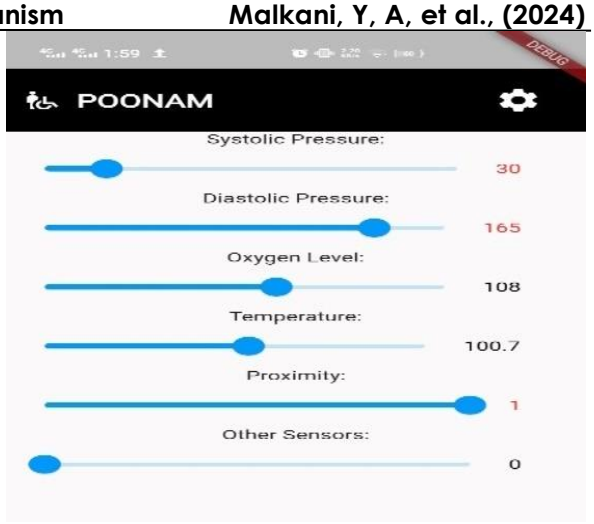


Figure 9.
(b): Sensor Widgets (Critical Condition)

(ii) Sensors Widgets: Figures 9 (a) and 9 (b) showcase the sensor widgets component, responsible for generating sensor data. Sliders enable real-time adjustment of sensor values, with critical thresholds highlighted in red when exceeded, as illustrated in Figure 9 (b).

(iii) Policies: The Policies component allows patients to manage their preferences and policies. These settings influence decision-making in the context matching mechanism. Figure 10 demonstrates how patients can configure these policies.

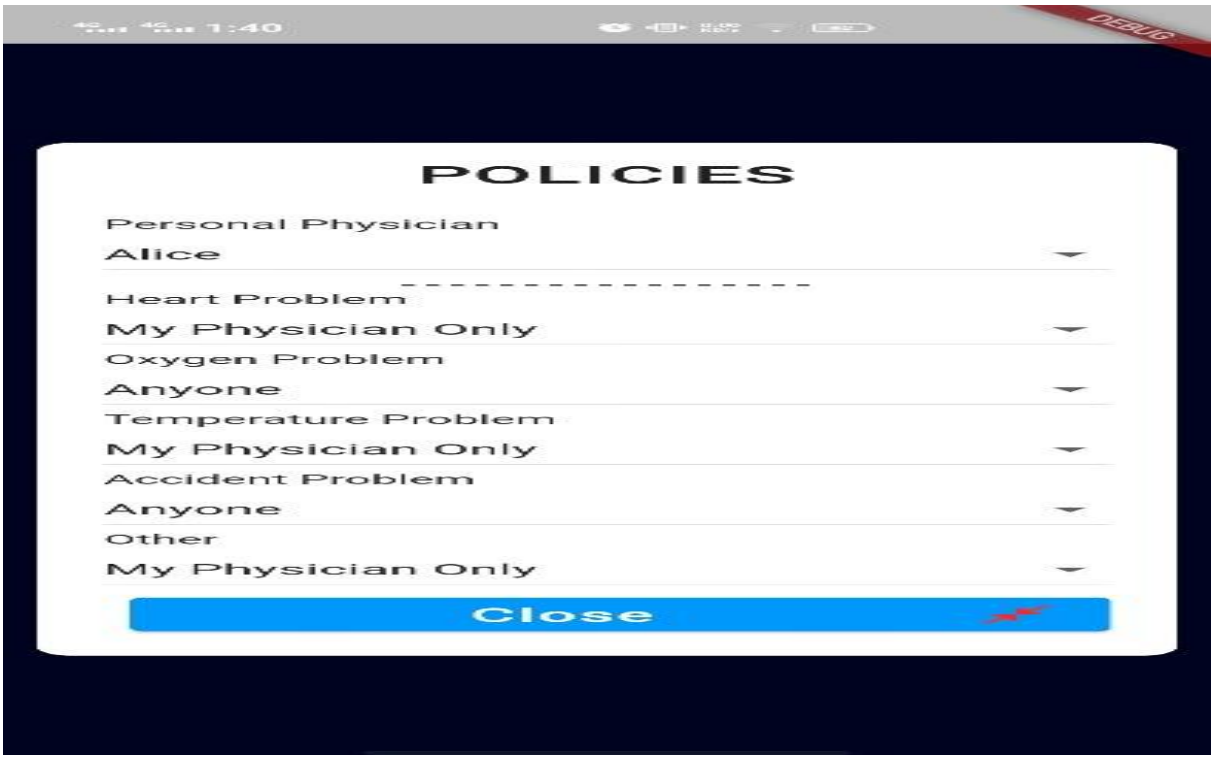


Figure 10.
Patient's application screenshot illustrating policies component

Doctor Application: The Doctor Application is tailored for use on IoT devices utilized by doctors, encompassing registration and patients discovery, and data fetch operation.

Figure 11.
(a): Doctor's Registration Screen

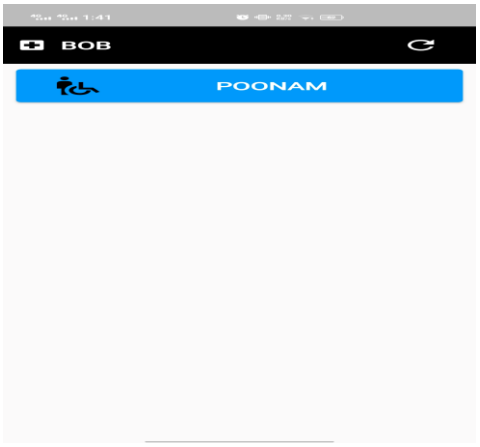


Figure 11.
(b): Patients Discovery Screen

Once registered, doctors can discover registered patients and their IoT devices. Access to data is granted based on credentials, contextual information, and patient-set policies. Figure 12 illustrates successful (Figure 12 (a)) and failed (Figure 12 (b)) data fetch operations. Access is denied when credentials are insufficient, demonstrating the system's robust security measures.

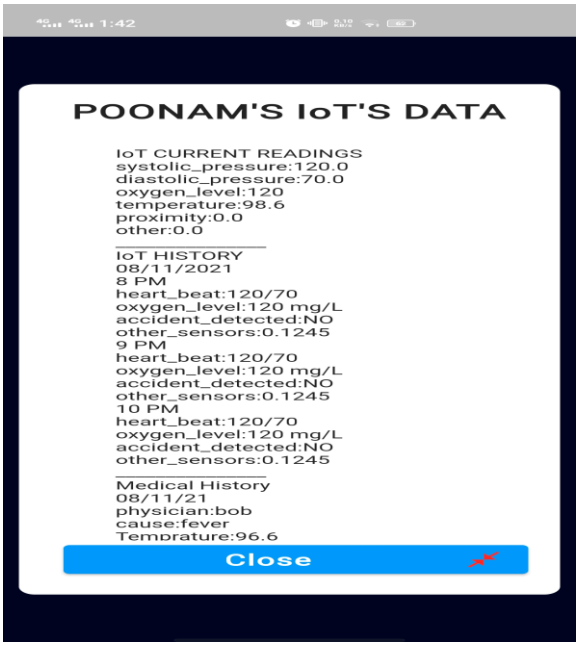


Figure 12.
(a): Screenshot of successful data fetch operation

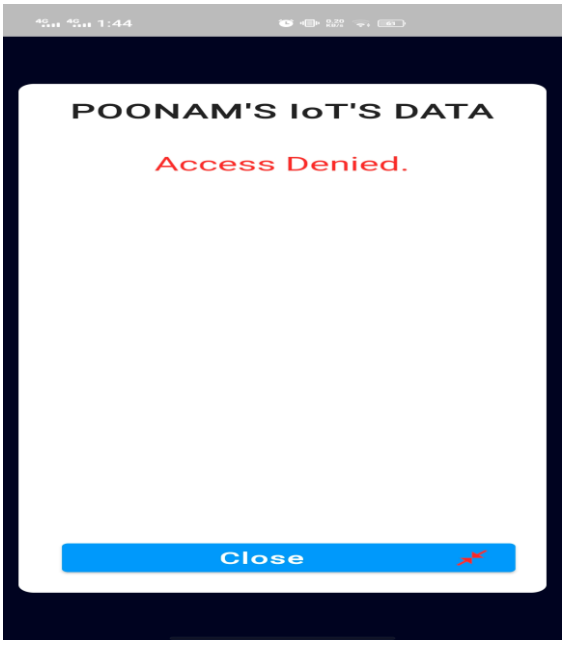


Figure 12
(b): Screenshot of failed data fetch due to insufficient credentials

The Server Application: Figure 13 shows the screenshot of server application. The server application operates as a console-based system with two synchronized components: the Request Response Manager (RRM) and the Context Matching Mechanism (CMM).

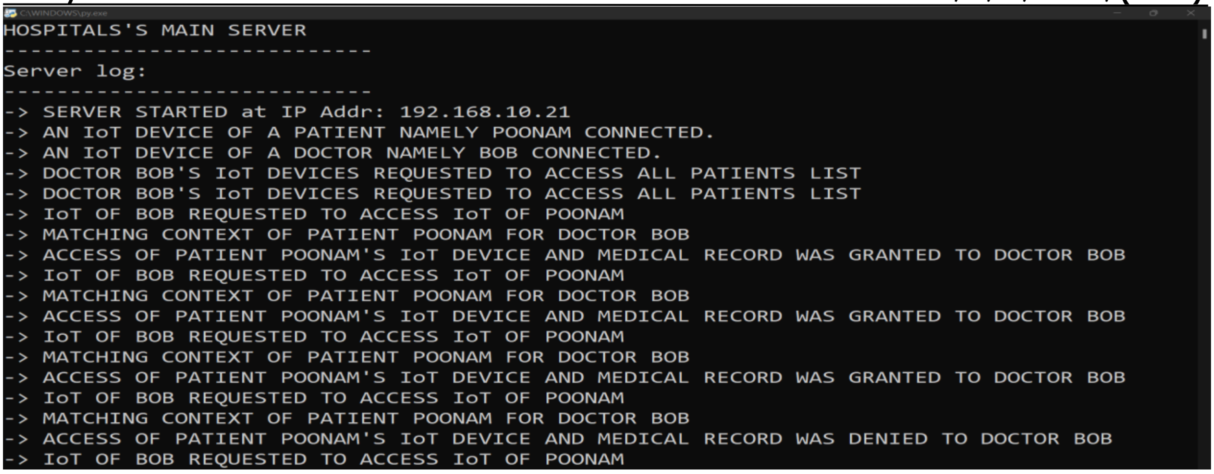


Figure 13.
Screenshot of the Server Application

The RRM is responsible for handling incoming requests, managing connections between devices and the server, and logging all system activities. Figure 13 provides an illustration of the server application's interface, showcasing logs and operational details to monitor the system's activities. CMM evaluates access requests by analyzing contextual information along with predefined policies and decides whether access permissions should be granted or denied.

RESULTS AND DISCUSSION

After successfully implementation and testing of the proposed access control system, a comprehensive usability study was conducted to evaluate the proposed system's performance and to determine its suitability for real world IoT environments. The usability study involved forty eight (48) participants. Table 1 shows the demographic information of these volunteer participants. In this usability study a 7-point likert scale (Malkani et al., 2013) is used to gather feedback from usability study participants, aiming to gauge user satisfaction and assess usability across different user roles and perspectives. This diversity ensured a comprehensive evaluation, capturing varied user experiences and expectations regarding the practical utility and effectiveness of the system.

Table 1.
Usability Study Participants' Profile Data

Gender:	**Nos.**	**%age**
Male	20	42%
Female	28	58%
Age:		
18 – 23	31	64%
24 – 28	6	13%
29 or above	11	23%
Last Qualification:		
Intermediate	2	4%
BS/MSc/MCS or Equivalent Degree	31	64%
MS/M.Phil	9	19%
PhD or above	6	13%
Occupation:		
Teaching	14	29%
Student	30	63%
Other	4	8%

This usability study was structured around the administration of two types of questionnaires (i.e. pre-test and post-test questionnaires) to measure the proposed system's usability. Pre-test questionnaire was used to collect the demographic information and profile details of the participants, ensuring a diverse representation of users involved in the study, while the post-test questionnaire was pivotal in gathering user feedback regarding their experience with the developed access control system. It included eight usability questions rated on a 7-point Likert scale, where 1 denoted the lowest satisfaction and 7 indicated the highest satisfaction level (Malkani et al., 2012).

As stated earlier, a total of 48 (forty eight) participants voluntarily took part in the usability evaluation, comprising students, teachers, and employees affiliated with the University of Sindh, Jamshoro. These participants were organized into twelve (12) groups, each consisting of four members, to facilitate structured feedback collection and rating of the system's usability. Figure 14 shows the snapshots taken while the participants were actively engaged with and using the proposed access control system. This figure also gives an overview of the usability study's practical setup and the interaction dynamics observed during the evaluation process.

Figure 14.
Usability evaluation participants while using the developed system

The results from the post-test questionnaire, as shown in Figures 15 to 18, depict the ratings given by each group across the eight usability questions. Each group's feedback was meticulously recorded and analyzed using spreadsheet software, MS

Excel, to generate detailed graphs (i.e. figures 15 to 18) that illustrate the distribution of ratings across different usability aspects. These figures segment the participant groups into subsets (Groups 1 to 3, Groups 4 to 6, Groups 7 to 9, and Groups 10 to 12), showcasing how each group rated the system's usability questions. This segmentation aids in identifying any variations or patterns in feedback across different user groups.

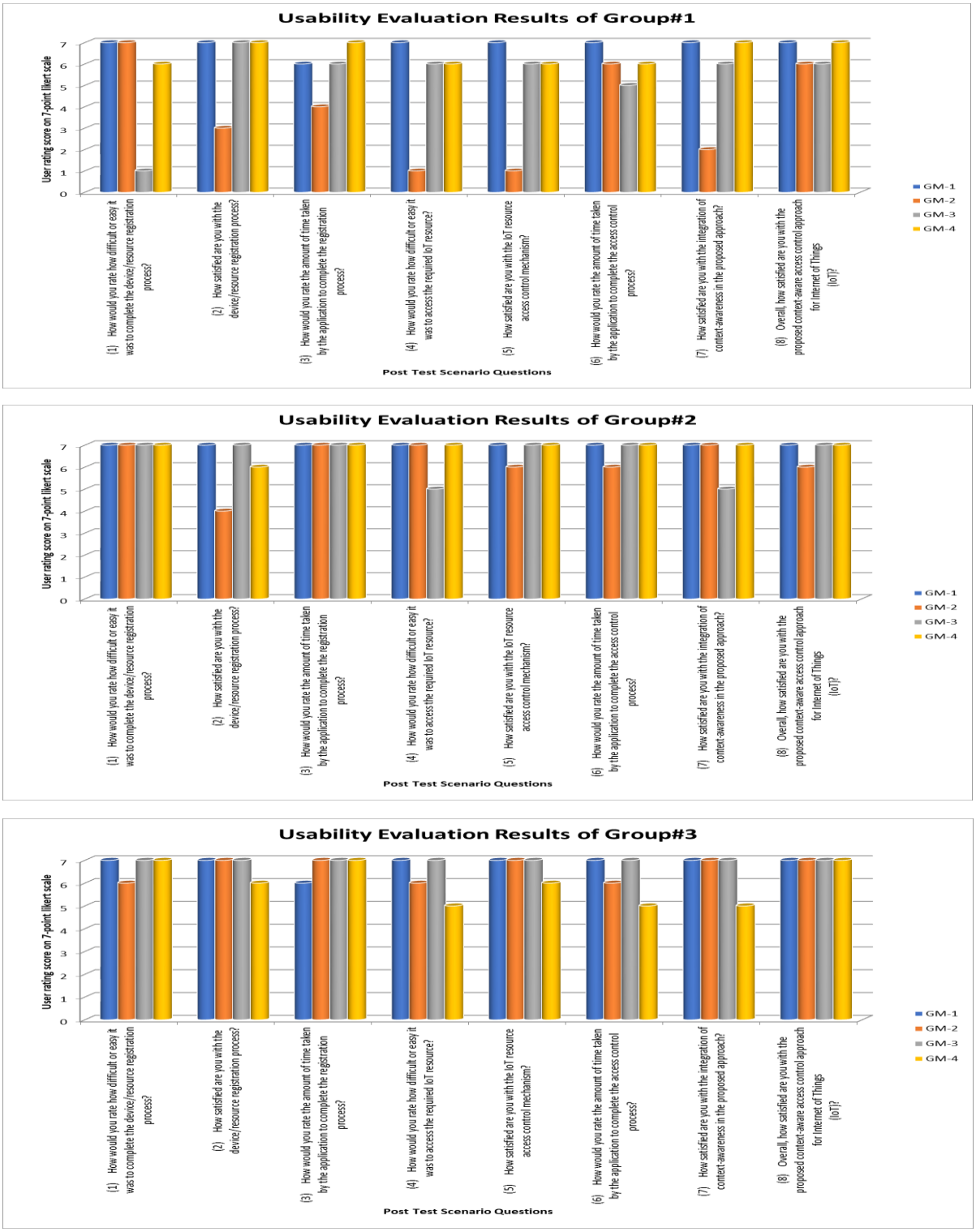


Figure 15.
Users given scores/ratings for 8 usability evaluation questions for groups 1 to 3

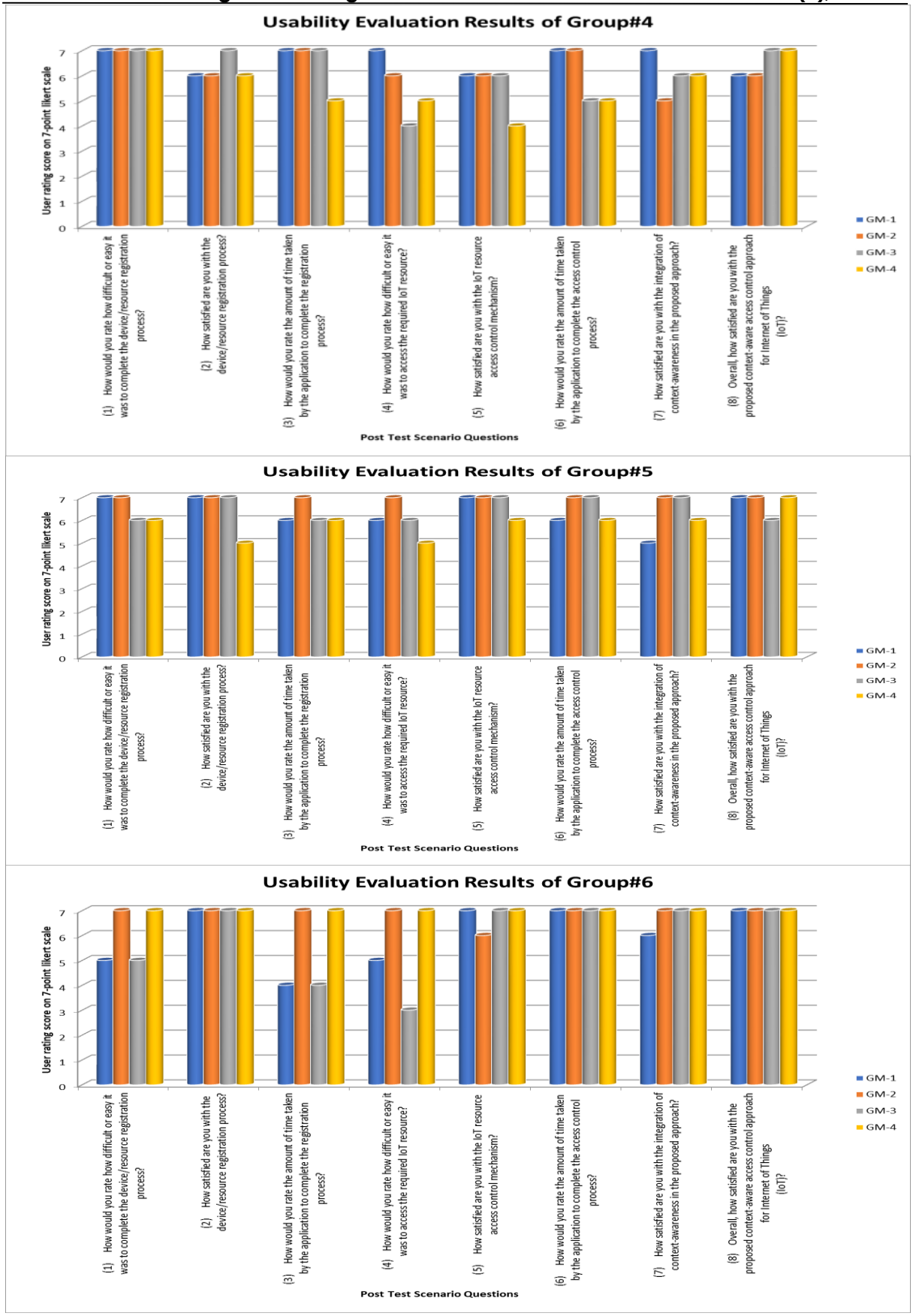
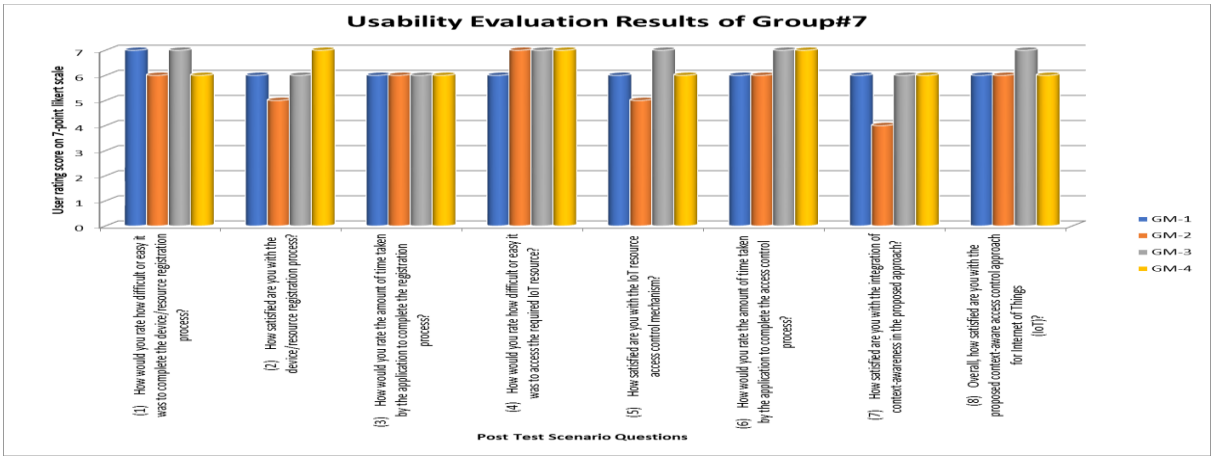
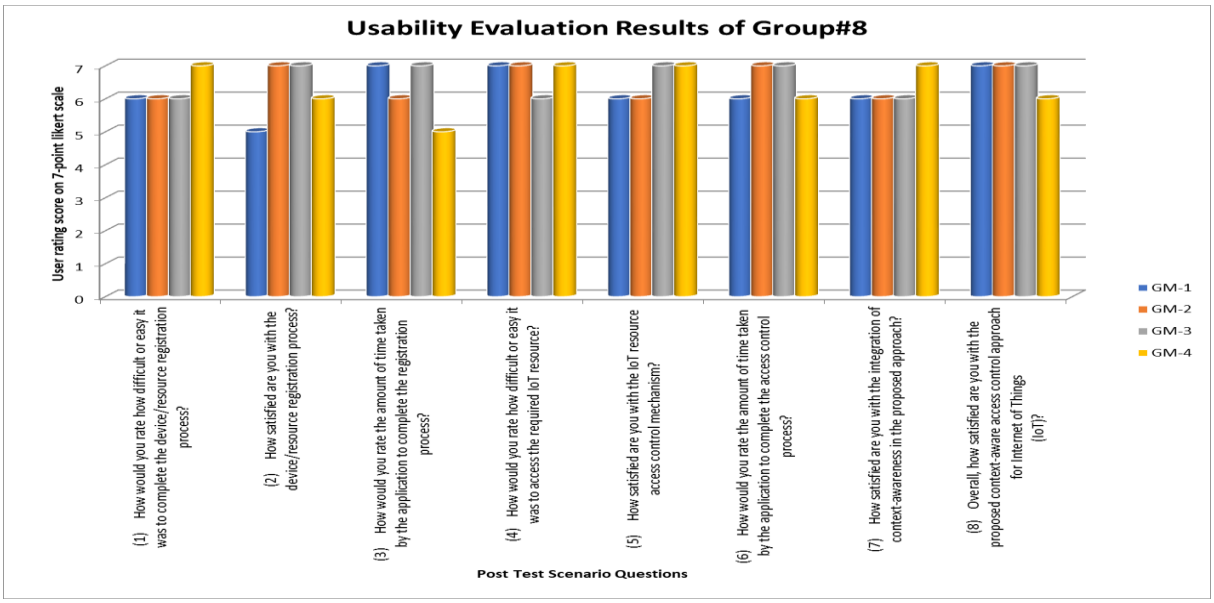


Figure 16.
Users given scores/ratings for 8 usability evaluation questions for groups 4 to 6





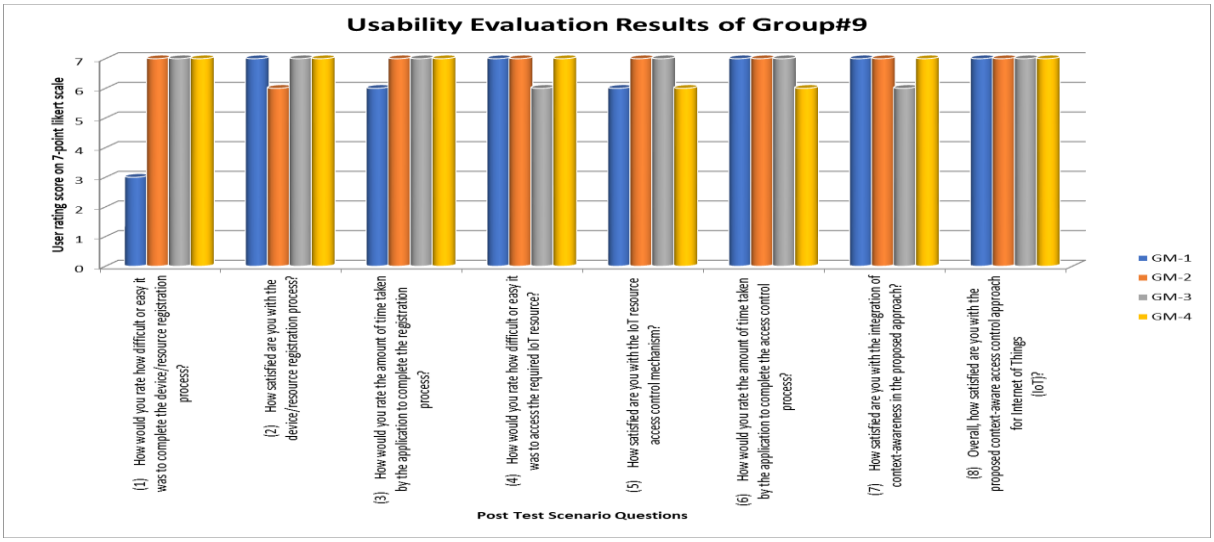


Figure 17.
Users given scores/ratings for 8 usability evaluation questions for groups 7 to 9

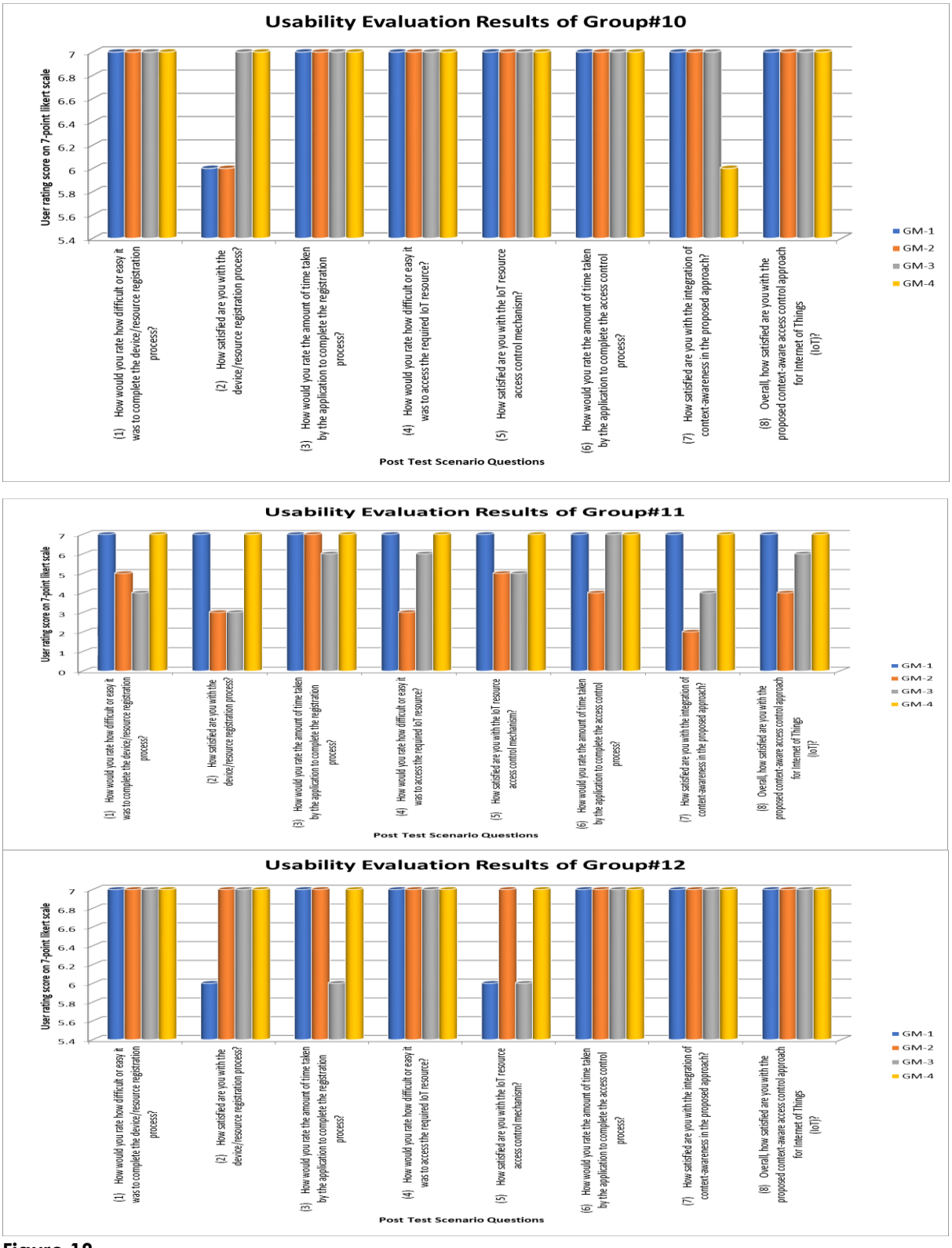


Figure 18.
Users given scores/ratings for 8 usability evaluation questions for groups 10 to 12

Table 2 consolidates the graphical data into a tabular summary, presenting the mean scores for each usability question across all participant groups. The mean scores, consistently at or above 6 for all questions, reflect a high level of user satisfaction and positive feedback regarding the system's usability. This aligns with established usability

evaluation standards (Stojkov et al., 2017; Malkani et al., 2021), indicating robust acceptance and effectiveness of the proposed access control solution for IoT environments.

Table 2.
The overall summarized results

	(1) How would you rate how difficult or easy it was to complete the device/resource registration process?	(2) How satisfied are you with the device/resource registration process?	(3) How would you rate the amount of time taken by the application to complete the registration process?	(4) How would you rate how difficult or easy it was to access the registered IoT resource?	(5) How satisfied are you with the IoT resource access control mechanism?	(6) How would you rate the amount of time taken by the application to complete the access control process?	(7) How satisfied are you with the integration of context-awareness in the proposed approach?	(8) Overall, how satisfied are you with the proposed context-aware access control approach for Internet of Things (IoT)?
group#1								
GM-1	7	7	6	7	7	7	7	7
GM-2	7	3	4	1	1	6	2	6
GM-3	1	7	6	6	6	5	6	6
GM-4	6	7	7	6	6	6	7	7
group#2								
GM-1	7	7	7	7	7	7	7	7
GM-2	7	4	7	7	6	6	7	6
GM-3	7	7	7	5	7	7	5	7
GM-4	7	6	7	7	7	7	7	7
group#3								
GM-1	7	7	6	7	7	7	7	7
GM-2	6	7	7	6	7	6	7	7
GM-3	7	7	7	7	7	7	7	7
GM-4	7	6	7	5	6	5	5	7
group#4								
GM-1	7	6	7	7	6	7	7	6
GM-2	7	6	7	6	6	7	5	6
GM-3	7	7	7	4	6	5	6	7
GM-4	7	6	5	5	4	5	6	7
group#5								
GM-1	7	7	6	6	7	6	5	7
GM-2	7	7	7	7	7	7	7	7
GM-3	6	7	6	6	7	7	7	6
GM-4	6	5	6	5	6	6	6	7
group#6								
GM-1	5	7	4	5	7	7	6	7
GM-2	7	7	7	7	6	7	7	7
GM-3	5	7	4	3	7	7	7	7
GM-4	7	7	7	7	7	7	7	7
group#7								
GM-1	7	6	6	6	6	6	6	6
GM-2	6	5	6	7	5	6	4	6
GM-3	7	6	6	7	7	7	6	7
GM-4	6	7	6	7	6	7	6	6
group#8								
GM-1	6	5	7	7	6	6	6	7
GM-2	6	7	6	7	6	7	6	7
GM-3	6	7	7	6	7	7	6	7
GM-4	7	6	5	7	7	6	7	6
group#9								
GM-1	3	7	6	7	6	7	7	7
GM-2	7	6	7	7	7	7	7	7
GM-3	7	7	7	6	7	7	6	7
GM-4	7	7	7	7	6	6	7	7
group#10								
GM-1	7	6	7	7	7	7	7	7
GM-2	7	6	7	7	7	7	7	7
GM-3	7	7	7	7	7	7	7	7
GM-4	7	7	7	7	7	7	6	7
group#11								
GM-1	7	7	7	7	7	7	7	7
GM-2	5	3	7	3	5	4	2	4
GM-3	4	3	6	6	5	7	4	6
GM-4	7	7	7	7	7	7	7	7
group#12								
GM-1	7	6	7	7	6	7	7	7
GM-2	7	7	7	7	7	7	7	7
GM-3	7	7	6	7	6	7	7	7
GM-4	7	7	7	7	7	7	7	7
Mean Score	**6.42**	**6.31**	**6.44**	**6.23**	**6.33**	**6.54**	**6.23**	**6.71**

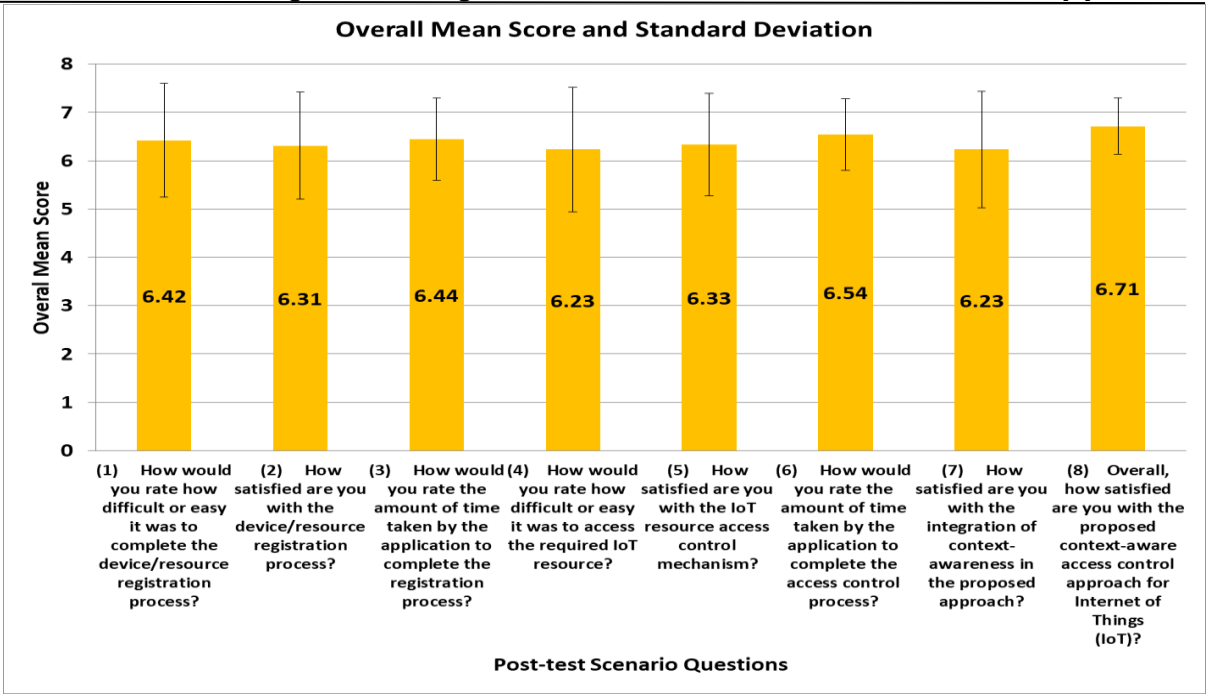


Figure 19.
Summary of overall scores/ratings including the mean and standard deviations

The culmination of the usability study for the proposed access control system in IoT is visually represented in Figure 19. This graph comprehensively displays the mean scores and standard deviations derived from feedback provided by all 48 participants involved in the study. According to the literature (Malkani et al., 2013; Stojkov et al., 2017; Nielsen & Levy, 1994), achieving a final mean score of 5.6 or higher on a 7-point likert scale signifies that a system or product is considered acceptable and usable from the users' perspective. In the case of the proposed access control system, the mean scores for all eight usability questions consistently exceeded 5.6. This indicates a strong level of satisfaction among participants regarding the system's usability. Therefore, based on the collected data and the established usability criteria, the proposed access control system emerges as a viable and effective solution for IoT scenarios requiring secure access management based on contextual information and policies. The positive feedback indicates the proposed system's potential to enhance user experience and operational efficiency within IoT environments.

CONCLUSION

Access control is an important component of computer security, which has been widely studied for several decades. Conventional access control approaches, such as RBAC, ACLs, and ABAC have their own strengths and weaknesses or limitations, particularly in the Internet of Things (IoT) landscape. For example, ACLs are effective in simpler environments with limited number of users and resources, but they struggle to scale in complex internet of things environments with a multitude of devices and users. The IoT environments, saturated with resource-constrained devices like mobile phones and sensors, poses unique challenges for access control. One major challenge is the dynamic nature of IoT environments, where access to resources needs to adapt in real-time rather than relying on static roles or rules. Addressing these challenges requires innovative access control approaches, specifically designed for IoT environments. Consequently, this research proposes a policy based contextual approach to access control in IoT, blending traditional access control approaches

with context-awareness and policy integration. The prototype of the proposed approach has been implemented and comprehensively tested, and a usability study is conducted in order to evaluate its practical application in IoT scenarios. The positive outcome from these evaluations indicates the potential of the proposed approach to enhance security and operational efficiency in dynamic IoT environments. Looking ahead, future enhancements could involve integrating numerous sources of real sensor data to enrich contextual information beyond the hypothetical scenario used in this study. Additionally, refining access policies using advanced policy management tools could provide more precise and adaptable control over access rights. These advancements aim to establish a robust foundation for securing IoT systems, paving the way for more resilient and scalable access control solutions tailored to evolving IoT environments.

DECLARATIONS

Acknowledgement: We appreciate the support from all the volunteers who took part in usability study that is carried out to evaluate the proposed approach.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: All volunteer participants of usability study were agree for publication of usability study results. All authors have given their consent.

REFERENCES

Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015). The Internet of Things (IoT): An Overview. International Journal of Engineering Research and Applications, 5(12, Part - 2), 71-82.

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999). Towards a better understanding of context and context-awareness. In Handheld and Ubiquitous Computing: First International Symposium, HUC'99 Karlsruhe, Germany, September 27–29, 1999 Proceedings 1, 304-307. Springer Berlin Heidelberg.

Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of Things Security, Device Authentication and Access Control: A Review. Journal of Cyber Security and Mobility, 14(8), 456-466.

Android Studio Home Page. (2024). An Overview of Android. Last accessed January, 2024, https://developer.android.com/studio

Ashton, K. (2017). Internet of Things Technologies – A Simple Explanation. Technource. https://www.technource.com/blog/the-internet-of-things-technologies-a-simple-explanation, last accessed on: June, 5, 2024.

Banafa, A. (2017). Three Major Challenges Facing IoT. IEEE Internet of Things. https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html

Barka, E., Mathew, S. S., & Atif, Y. (2015). Securing the Web of Things with Role-Based Access Control. In P. Samarati (Ed.), Data and Applications Security and Privacy XXIX (pp. 14-26). Springer International Publishing.

Bertin, E., Hussein, D., Sengul, C., & Frey, V. (2019). Access control in the Internet of Things: a survey of existing approaches and open research questions. Annales des Telecommunications, 74(7-8), 375-388.

Cerf, V. G. (2015). Access Control and the Internet of Things. IEEE Internet Computing, 19(5), 96.

Gerber, A. (2019). Top 10 Security Challenges of IoT. IBM Developer. https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/

Godha, R., Prateek, S., & Kataria, N. (2014). Home automation: Access control for IoT devices. International Journal of Scientific and Research Publications, 4(10), 1-5.

Guillemin, P., & Friess, P. (2009). Internet of Things Strategic Research Roadmap. The Cluster of European Research Projects, Tech. Rep.

Gusmeroli, S., Piccione, S., & Rotondi, D. (2012). IoT Access Control Issues: A Capability-Based Approach. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 787-792.

Jayant, B. D., & Sulabha, A. S. (2014). Analysis of DAC, MAC, RBAC Access Control based Models for Security. International Journal of Computer Applications, 104(5), 975-8887.

Jindou, J., Xiaofeng, Q., & Cheng, C. (2012). Access control method for web of things based on role and SNS. 2012 IEEE 12th International Conference on Computer and Information Technology (CIT), 316-321.

Kumar, P., & Pati, U. C. (2016). IoT Based Monitoring and Control of Appliances for Smart Home. Pre-print version, IEEE Transactions.

Kuyoro, S., Osisanwo, F., & Akinsowon, O. (2015). Internet of Things (IoT): An Overview. In Proceedings of 3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM-2015) (pp. 1-8). London, UK.

Lashkov, A. (2019, August 6). Access Control Models: Review of Types and Use-Cases. Medium. https://medium.com/yellow-universe/access-control-models-review-of-types-and-use-cases-1f4c427b0cc2

Liu, J., Xiao, Y., & Chen, C. L. P. (2012). Authentication and Access Control in the Internet of Things. In Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW'12), Macau, China, 588-592. IEEE.

Liu, Q., Zhang, H., Wan, J., & Chen, X. (2017). An Access Control Model for Resource Sharing Based on the Role-Based Access Control Intended for Multi-Domain Manufacturing Internet of Things. IEEE Access, 5, 7001-7011.

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability-based access control (IACAC) for the internet of things. Journal of Cyber Security and Mobility, 1, 309-348.

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2012, September). Identity Establishment and Capability based Access Control (iecac) scheme for Internet of Things. In Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications (WPMC'12), Taipei, China, 187-191. IEEE.

Malkani, Y. A., Keerio, A., & Dhomeja, L. D. (2012). Secure Device Pairing: A Usability Study. International Journal of UbiComp (IJU), 3(2), 18-27.

Malkani, Y. A., Keerio, A., & Mahesar, A. W. (2013). Performance and Usability Analysis of Proof-of-Proximity (PoP) Framework. Sindh University Research Journal (SURJ), 45(4), 89-95.

Malkani, Y. A., Malik, M. A., Dhomeja, L. D., Mahessar, A. W., & Memon, B. R. (2021). A QR Code Based Group Pairing Approach for Mobile Ad Hoc Networks. Sukkur IBA Journal of Computing and Mathematical Sciences (SJCMS), 5(1), 24-35.

Nielsen, J., & Levy, J. (1994). Measuring usability: preference vs. performance. Communications of the ACM, 37(4), 66-75.

OpenID Home Page. (2019). What is OpenID? https://openid.net/what-is-openid/

Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2016). Access Control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 96, 10-22.

Rajpoot, Q., Jensen, C., & Krishnan, R. (2015). Integrating Attributes into Role-Based Access Control. In P. Samarati (Ed.), Data and Applications Security and Privacy XXIX (Lecture Notes in Computer Science, vol 9149). Springer, Cham.

Remote Patient Monitoring Tools / Devices. (2017). Last retrieved on June, 5, 2024 from http://toolanddevices.blogspot.com/

Salama, U., Yao, L., Wang, X., Paik, H. Y., & Beheshti, A. (2017). Multi-Level Privacy-Preserving Access Control as a Service for Personal Healthcare Monitoring. 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, 878-881.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks, 76, 146-164.

Soomro, A. K. (2019). Supporting Policy-Based Contextual Adaptation in Service Discovery Protocols (MPhil thesis). IICT, University of Sindh, Jamshoro, Pakistan.

Stojkov, M., Milosavljević, B., & Sladić, G. (2017). On the Usability of Access Control Models in IOT. 8th PSU-UNS International Conference on Engineering and Technology (ICET), June 2017.

Yuan, E., & Tong, J. (2005). Attributed based access control (ABAC) for Web services. 2005 IEEE International Conference on Web Services (ICWS), 561-569.

Zhang, G., & Gong, W. (2011). The Research of Access Control Based on UCON in the Internet of Things. Journal of Software, 6(4), 724-731.

Zhang, G., & Liu, J. (2012). The Study of Access Control for Service-Oriented Computing in Internet of Things. International Journal of Wireless and Microwave Technologies (IJWMT), 2(3), 62-68.

Zhang, G., & Tian, J. (2010). An extended role based access control model for the internet of things. 2010 International Conference on Information, Networking and Automation (ICINA), 1, IEEE, V1-319.

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's Intranet of things to a future Internet of things: a wireless- and mobility-related view. IEEE Wireless Communications, 17(6), 44-51.