Risk Monitoring for Confidentiality of Healthcare Data

Ahmed F. Siddiqui[1], Aditya J. Paul[1], Sushruta Mishra[1]

[1]*Kalinga Institute of Industrial Technology, India*

Abstract

The Internet of Medical Things (IoMT), the newest component of the Internet of Things, offers uses for intelligent healthcare systems. It is crucial to the healthcare industry's efforts to improve the accuracy, reliability, and efficiency of electronic devices. IoMT can connect genuine, physical items in the real world for information sharing and communication. Therefore, it is crucial to utilize access control to guarantee the proper use of private data during the data sharing process. In this research paper we have tried to discuss three cutting edge access based control mechanisms in a comparative fashion to understand and overcome the limitations of the classical access control methods. The healthcare industry's future regarding their risk monitoring strategies was also covered in this research paper.

Keywords

Internet-of-Medical-Things(IOMT), Risk Monitoring, Healthcare, Sensors, Privacy, Access Control, SADAC, MLS-ABAC, DF-RBAC-SC

1. Introduction

The Internet-of-Medical-Things (IoMT) [1], [2] applies the Internet-of-Things (IoT) to the medical and healthcare sectors by using edge computing and big data analytics to identify trends in medical datasets and by connecting medical resources and services via a variety of network services. The introduction of IoMT has made it possible to realize the link between medical personnel, patients, and numerous pieces of medical equipment, giving patients with high-quality equipment assistance at any time and location. To gather health data, sensor devices are placed into the bodies of patients [3, 4, 5]. These gadgets include sensors for weight, blood pressure, temperature, and heart rate. After using this data for analysis, the user selects a pertinent diagnosis scheme for diagnosis based on the analysis' findings. In this manner, a contact-less patient diagnostic working paradigm is described.

Users may perform real-time interactions anytime, anyplace, and from any location to benefit from services like tele-care because of the intelligent nature of IoMT networks and the openness of its related applications. There are clearly issues with information security and privacy due to this instant connectivity. It is crucial to regulate user behavior based on different access levels, or a multi-level access control method. For instance, access to the information in a healthcare network is restricted to authorized entities that meet the access control requirements (e.g., roles and resources).

Access control is a key security feature that ensures that, when certain environmental criteria are met, only authorized subjects have access to particular resources for a given activity [6]. The four components that make up this concept are subjects (such as people or devices), resources or objects (such as web pages, bank accounts, or database records), actions (such as read, write, and execute), and environmental factors (e.g., date, location).

The concepts and principles of access control implementations were introduced by Sandhu et al. in 1994 [6], who also described many models that serve as the foundation for the majority of contemporary access control implementations. [7]

International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT 2023), May XX-XX, 2023, Delhi, India

EMAIL: ahmedfarazsiddiqui1@gmail.com (A. F. Siddiqui); 2005986@kiit.ac.in (A. J. Paul): sushruta.mishrafcs@kiit.ac.in ((S.Mishra)
ORCID: 0000-0003-3929-1100 (S.Mishra)

Table 1
Comparison between original access control models

Access control method	Basis of permission allocation	Access control decision-maker	Advantages	Disadvantages
DAC	Access control matrix and access control list (ACL)	Data Owner	Easy to manage, search, authorization.	When faced with complex environments, multiple ACLs are required and difficult to manage.
MAC	Security Level	Central Organization	Meet multi-level security requirements.	Flexibility is poor.
RBAC	Role	Central Organization	Simplify access management.	It is easy to cause character explosions.

2. Objectives of the Paper

The objectives of the study are mentioned below:-

- Determining the security issue with the healthcare industry's data sharing and storage methods as well as the goals of the suggested solution.
- Comparison and defining three different access control models for healthcare.
- Explaining the design of the access control models through a scenario of the healthcare context.
- Discussing about the use, ramifications, and the potential of the suggested strategy in future.

3. Related Works

Most studies focus primarily on two aspects: encryption and access control, in order to prevent unwanted access while guaranteeing data confidentiality, in order to address the issues of privacy leaks created by centralized cloud storage. Conventional access control techniques, like Discretionary Access Control (DAC) [8], put the user first. The data owner creates access policies, and an access control matrix and access control list are used to implement access control (ACL). However only basic environments are appropriate for this technique. Using static ACL, users may quickly query and control personal resources. Nevertheless, this approach is only appropriate in straightforward environments. More ACLs are required for remote environments where user rights frequently change, and it is challenging to maintain. Via the central authority, Mandatory Access Control (MAC) [9] distributes the subject's and object's access permissions in accordance with the security level. As a result, once the security level is established, the access privileges follow suit. Consequently, the largest drawback of strict access control is its lack of flexibility. RBAC [10] is a technique for allocating access privileges to subjects in accordance with their jobs. Limited roles can represent several users, which simplifies the administration of authority between the subject and the object. But the conventional approach to role-based access control is typically centralized, the distribution of user roles lacks fine granularity, and the distribution of roles and permissions is static, which is incompatible with the modern dispersed and dynamic network design. As a result, DF-RBAC was conceptualized, a dynamic and fine-grained role-based access control model that enables resource proprietors to designate roles in a flexible manner while also ensuring the security of those roles [11].

The shortcomings of static authorization in the case of RBAC are efficiently solved by Attraction-based Access Control (ABAC) [12], a fine-grained and dynamic access control mechanism. It is a versatile access control mechanism since it grants users access privileges in accordance with qualities and supports complicated contexts. The National Institute of Standards and Technology (NIST) provided a comprehensive ABAC guide in 2014, and it was updated in 2019 through [13]. This document begins by defining it and outlining the many parts that make it work. Second, it talks about how ABAC is put into practice within a company. The guide's primary goal is to illustrate the key difficulties that arise throughout such an implementation.

Data confidentiality is not provided by the ABAC paradigm. The MLS-ABAC model, which not only functions using the original workflow of the regular ABAC model but also assures data secrecy, was developed to address this flaw [14]. There ABAC implementations have been used in cloud storage and the Internet of Things [15], [16], [17], [18], [19], [20], where the use of blockchain technology is recurrently considered to prevent data from manipulation or unauthorized access [21], [22], [23].

Similar to ideas like "software as a service" or "malware as a service," security as a service (SECaaS) has gained popularity in recent years [24], [25]. SECaaS is a business strategy in which a service provider incorporates security services into a company infrastructure more efficiently than the majority of people or businesses can do on their own (typically on a subscription basis). In this context, SADAC (Security Attribute-based Dynamic Access Control), a novel method for dynamic access control based on the subject's security attributes, was presented and is primarily meant to be used in business networks and environments linked to ISPs [26].

4. Comparative Analysis of three access control models

In this section, we shall discuss the various features of the following models:

- SADAC(Security Attribute-based Dynamic Access Control)
- MLS-ABAC(Multilevel Attribute-based Access Control)
- DF-RBAC-SC(Dynamic and Fine-grained Role-based access control using Smart Contracts)

4.1.SADAC(Security Attribute-based Dynamic Access Control)

SADAC (Security Attribute-based Dynamic Access Control)[26] is a novel zero-trust network access control scheme that collects (i) multiple security-related attributes about communications (such as ports, IP addresses, data volume, and duration), applications installed and permissions involved, resource consumption (such as RAM, CPU, and battery) and device protection mechanisms (such as screen locking method); (ii) uses these attributes over time to authorize or deny access in a dynamic, continuous manner. and (iii) the ML scheme that supports SADAC (MSNM) presents diagnosis capabilities to allow identifying specific causes for access restrictions. The general operational workflow shown in Figure 1.

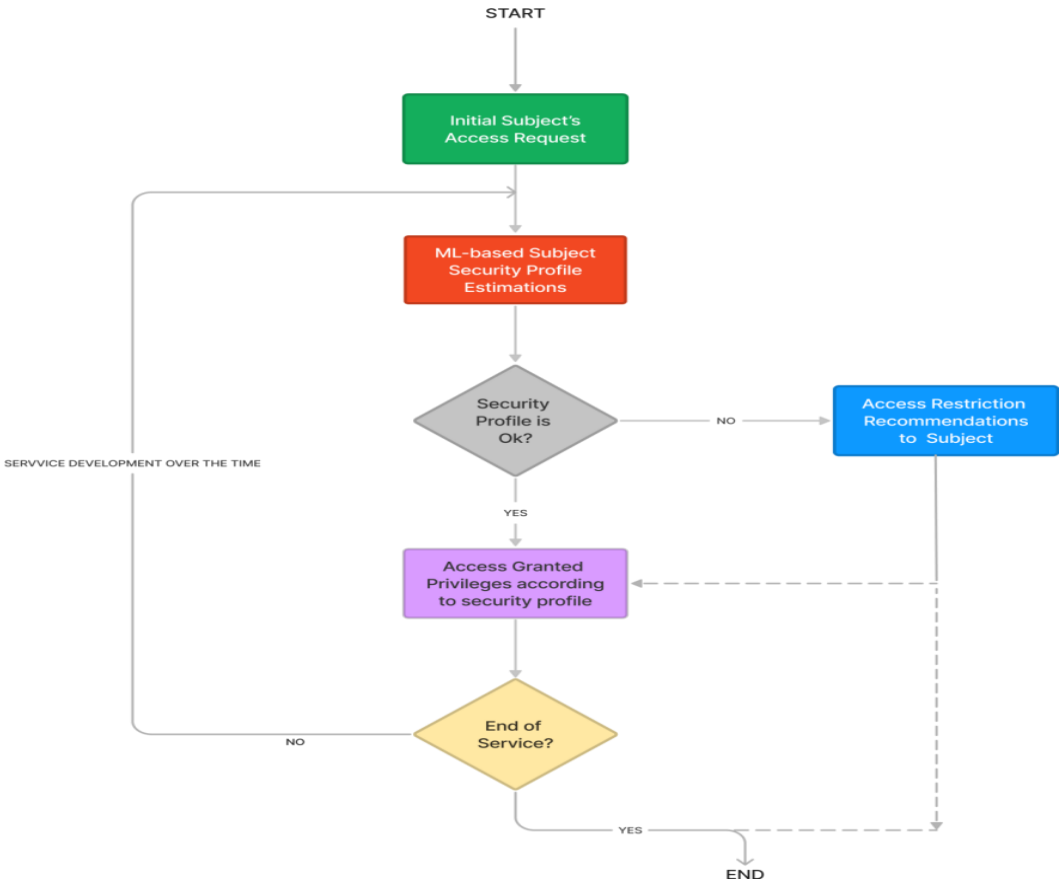

Figure 1: General operational workflow of SADAC

We shall understand this through an example of a device in a WiFi environment: Through an Access Point, each mobile device communicates with the surroundings (AP). This kind of engagement is deceptive. On the one hand, a mobile-network discussion is conducted in order to manage the access itself. Nonetheless, the device offers the network some particular security features or properties. The usage of a SADAC-specific app, which may be downloaded from the ISP network and installed on the device, makes this process easier.

The AP implements the dPEP module, so that:

- It obtains the security features connected to a certain device or user, which can be done either once at the time of association with the AP or repeatedly over time.
- The dPDP will determine the appropriate security profiles for the device/user based on the security features that the AP has forwarded to it.
- If the dPDP determines that a particular device or user is not complying with a security policy, it instructs the AP/dPEP to restrict or even forbid the device from continuing to access the network.

Each mobile device's security profile is estimated by the dPDP module using the related security attributes. Also, it will decide whether to expand or restrict network access. Both the security policy repository created for the environment and the repository of security attributes for the network's connected devices are taken into account in order to accomplish this [27] [28].

SADAC is capable of diagnostics and is based on security. Additionally, it can be combined with the usage of additional traits and circumstances, whether or not they are security-related, to make more complicated and ambitious access control decisions. Moving the estimation and diagnosis modules to the final devices would also make it simple to expand it in order to strengthen user privacy. The security profile of people and devices should be taken into account as a confidence measure to allow access to ICT environments, despite the sensitive nature of the problem itself and the potential remedies to be adopted.

4.2.MLS-ABAC(Multilevel Attribute-based Access Control)

MLS-ABAC(Multilevel Attribute-based Access Control) scheme[30], the cloud server first determines the data user's security level, then searches the database based on the security level.

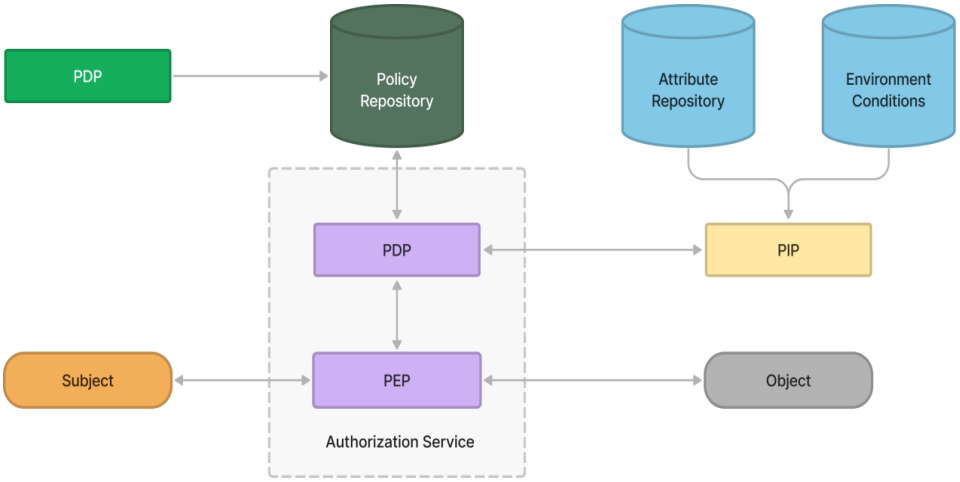

Figure 2: NIST's ABAC model

NIST's ABAC Figure 2 The model is satisfied by the Multi-Level Security ABAC (MLS-ABAC) scheme. This design is effective and is based on the Ciphertext-Policy ABE decryption technique. Furthermore, based on actual application circumstances, only authorized data users are able to decrypt the ciphertext and verify the message's integrity after retrieval.

Anything that is transferred to the cloud that is sensitive (such as medical records) should be securely kept (i.e. encrypted). The data should only be readable by an authorized user who possesses the security key. As a result, incorporating ABAC into Attribute-Based Encryption (ABE) gives us the opportunity to encrypt the information that has been outsourced and shield it from the cloud system itself. Even if a cloud system were sincere and curious, it would be impossible for it to access the private data using ABE Figure 3 depicts the MLS-ABAC architecture.

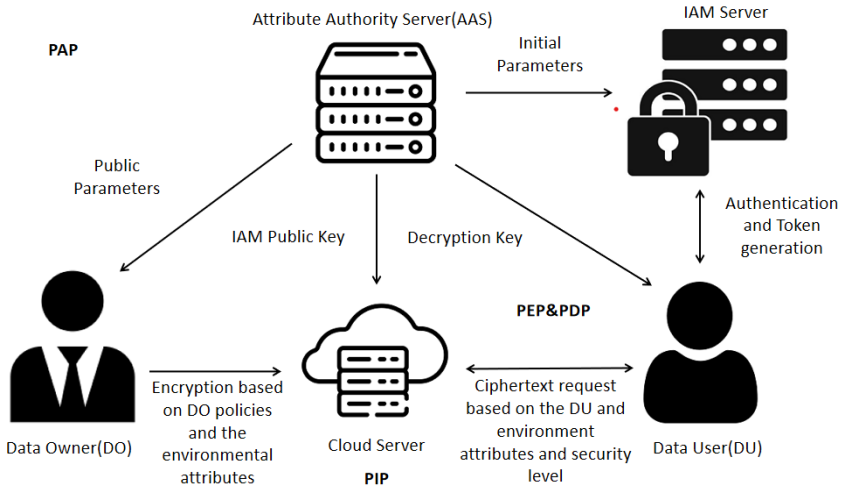

Figure 3: MLS-ABAC model

- Attribute Authority Server (AAS) - It is a dependable party that creates both the secret keys and system parameters for the data users.
- Identity and Access Management Server (IAMS) - Based on sets of security levels, the Identity and Access Management Server (IAMS) generates tokens for users corresponding to their access security level. Notably, these sets are created, deleted, and updated by AAS, who then submits them to the IAMS.

- Cloud Server (CS) - In order to store ciphertexts that are offloaded from IoT data providers, the Cloud Server (CS) functions as a repository. As a data consumer, CS also verifies the authenticity of the tokens it has obtained from another IoT device. The defined predicate functions are then used by CS to determine whether access should be permitted.
- Data Owner(DO) - By specifying a security level, Data Owner (DO), an IoT data producer, can share a sensitive message with consumers. In order to achieve this, it creates a ciphertext that also contains certain metadata. Consequently, in order to stop data leaking, the DO selects the ciphertext's security level and uploads the ciphertext together with the corresponding security level to CS.
- Data User(DU) - A lightweight IoT device called Data User (DU) wishes to read data from the CS using its credentials (i.e., data consumer). It communicates the token to CS after requesting one from the IAMS in order to accomplish this. The DU can get the ciphertext if it successfully completes the verification process. Lastly, the DU can decrypt the ciphertext to discover information if its properties meet the access policy. Otherwise, it learns nothing.

We shall explain the methodology with an example of a hospital: In Figure 4, the set of static characteristics is {UserType, HospitalId}, while the set of dynamic attributes is {Section, Time}. The four security levels in our suggested paradigm are Top Secret, Secret, Confidential, and Unclassified, with User A belonging to Security Level Secret. User A belongs to the security level Top Secret, User B and User C to Secret, User D and User E to Confidential, and User F to Unclassified. Users are given this partial order hierarchy by the system administrator (in this case, IAMS), who also notifies them when the system's rules change[29].

In this system, the entity User E has the ability to download information that has been uploaded with Confidential and Unclassified security levels, as well as to decrypt information that has been encrypted with User E's static and dynamic properties. Additionally, if User E's security level is raised to Secret, it will be able to download any material posted to security levels Secret and lower and decode any information that has been encrypted using the static and dynamic characteristics of the application. According to the aforementioned situation, the system administrator can easily grant User E access to the wrapped data that has been uploaded to the Confidential security level.

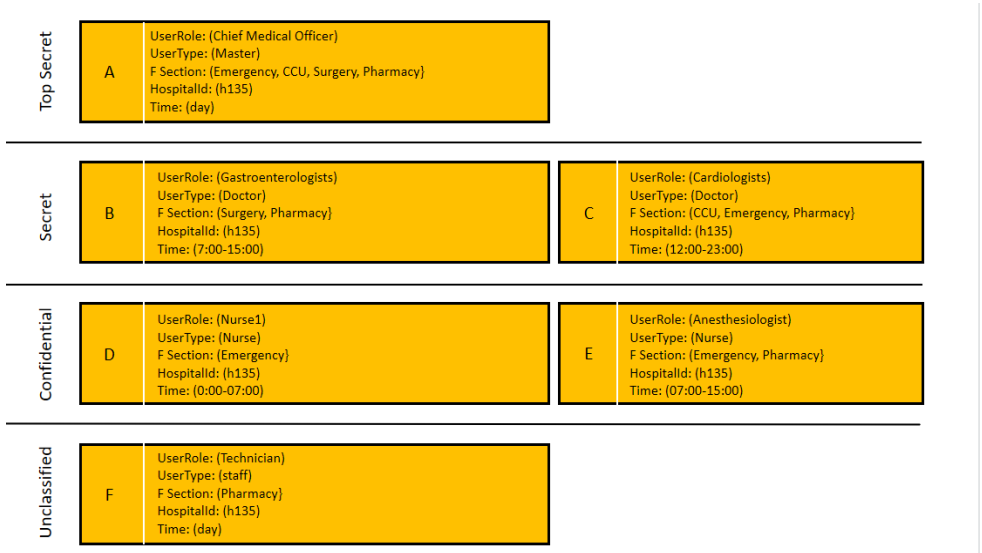

Figure 4: Multi-level Security with ABAC Example

The management of access control is made easier and the security and privacy of IoT systems are improved by adding a security level verification before partial decryption. MLS-ABAC is effective when lightweight alternatives to heavyweight functions are used, such as the suggested lightweight CP-ABE[30], lightweight Ascon-hash, and Ascon[29],[31], authenticated encryption algorithms. In addition to taking security level verification and dynamic attributes into account, MLS-ABAC uses an authorized encryption strategy to safeguard the data integrity of the plain text in the event of outsourced

decryption. As an added bonus, it formalizes the suggested access control model by including a conceptual and formal model as well as performance metrics to illustrate the use-case and implementation of the MLS-ABAC scheme.

4.3.DF-RBAC-SC(Dynamic and Fine-grained Role-based access control using Smart Contracts)

Using DF-RBAC-SC(Dynamic and Fine-grained Role-based access control using Smart Contacts) [32] [33] [34] we can verify the user-role assignments of organizations in a secure way in a cross-organizational setting. DF-RBAC-SC is a smart contract-based authentication mechanism that is suitable for the trans-organizational exploitation of roles, in order to accomplish these objectives. A challenge-response protocol and a smart contract make up the two primary components of the DF-RBAC-SC. The user-role assignments are made using the smart contract (SC), which is subsequently broadcast on the blockchain. Figure 5 depicts the DF-RBAC-SC access framework.

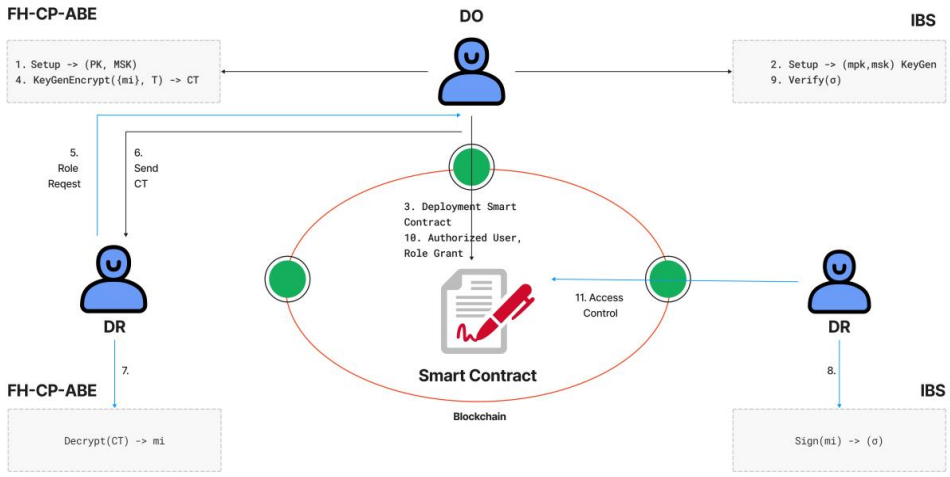

Figure 5: Flow chart of access framework of DF-RBAC

We shall explain the methodology using an example of a hospital: Imagine that a hospital (A-Hospital), a role-issuing entity, wants to administer a "patient" role for its patients. The RBAC-smart SC's contract would then be made and published on the Ethereum network. Utilizing the clever contract, it may carry out a command to add a user (patient) to the database. In addition to the role that will be assigned to the patient, A-Hospital will also include the patient's externally owned address (EOA), the role's expiration date and any other personalizations. The user then claims to have the patient's position from A-Hospital and asks for a service from a service-providing company such as a pathology lab.

The service provider(pathology lab) checks the smart contract made by A-Hospital based on the claim and uses that to verify all the facts it requires. Following a thorough review of all the information, the hospital can use the challenge-response protocol to determine whether the unknown user has access to the corresponding EOA that was given the role, conclusively demonstrating that the unknown user was, in fact, given a patient role by A-Hospital. Because the information the hospital needs is available publicly or is already in the user's possession, it is important to note that the hospital does not need to be aware of the role in advance and is not required to enter into any agreements with or contact A-Hospital on behalf of the patient who received the role.

It is suggested to use DF-RBAC-SC with cryptography. This framework enables the resource owner to assign user responsibilities in a flexible manner. At the same time, it may confirm the roles that have been allocated, carry out the function of accessing the activity log for security audit purposes, and guarantee the security of the entire architecture. It has demonstrated through safety and experimental research that our framework is workable.

5. Future scope of healthcare informatics

The digital transformation has only steadily and graciously affected the medical industry [35].High-end sensors and other similar devices are being used in smart hospitals and related environments to generate and gather massive volumes of extremely complicated medical data in real-time with demanding data processing needs. The growth of AI and the internet of medical things (IoMT) as well as the advent of digital health care reforms has been closely related. These systems, also known as health care IoT, are made up of a networked arrangement of medical devices—mostly sensors and small-scale devices—and software programmes that enable communication across various software-based healthcare systems [36].

When it comes to managing medical records, the health care sector has already experienced a significant level of digitization in the form of electronic health records (EHR) [37]. The bulk of the pharmaceutical and related sectors already use digital datasets or cloud-based systems to start electronic record-keeping for massive amounts of organizational and research data. The term "edge computing" (EC) is a new one, but it has the ability to fully address the needs relating to system reaction times and data privacy protection [38]. It serves as a framework for adding privacy protection and a means for lessening load in server-based solutions. The "man-in-the-middle" function is often performed by the edge server, which also serves as an instantaneous query and data management system and only connects to the server for high priority or high complexity tasks [39]. Many attempts are being undertaken to study and broaden EC's reach into closely linked and related sectors, wherever there is potential for distributed architecture, as a result of substantial research being done in this area. As a result, many distributed learning models have been developed, including Edge intelligence [40], distributed learning, and federated learning.

6. Conclusion

These days, ICT security is of the utmost importance. The upcoming use of technologies like IoT(Internet of Things) and BYOD(Bring Your Own Device) will make this scenario even worse. The security profile of the subjects in healthcare system (devices/users) is dynamically evaluated in order to allow, limit, or refuse access to services and resources of the network over time, in light of the growing relevance and impact of security threats. We intended to provide a deep insight into some of the access control models that can be used to identify risks of data leak and privacy loss in the healthcare industry as the data is sensitive, personal and very detailed.

We can conclude that among DAC, MAC, RBAC we prefer RBAC as it is a great combination of both DAC and MAC and it gives us the best of both worlds. RBAC is an intermediate model between MAC and DAC, as it provides greater flexibility than MAC while it is more manageable than DAC. This has boosted the acceptance of RBAC in the corporate world. Hence we discussed the three most suitable models under RBAC i.e. SADAC, MLS-ABAC, DF-RBAC-SC for a healthcare system that can help us protect sensitive information and identify risks and deal with them.

7. Acknowledgements

I would like to extend my heartfelt appreciation to everyone who helped make this research effort a success. First and foremost, I would like to express my sincere gratitude to Dr. Sushruta Mishra who served as my research guide for the study for all of his tremendous support. Also want to express my gratitude to my co-author Ahmed Faraz Siddiqui, who worked with me on the studies and paper preparation. .

8. References

[1] Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput Commun 166. (2021):110-124.

[2] Kumar M, Verma S, Kumar A, Ijaz MF, Rawat DB, et al. ANAF-IoMT: A novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC. IEEE Trans Ind Inform 18(12). (2022):8936-8943.

[3] Wang R-B, Wang W-F, Xu L, Pan J-S, Chu S-C. Improved DV-hop based on parallel and compact whale optimization algorithm for localization in wireless sensor networks Wirel. Netw. (2022):1-18.

[4] Chen C-M, Chen Z, Kumari S, Lin M-C. LAP-IoHT: A lightweight authentication protocol for the internet of health things Sensors 22(14). (2022):5401.
[5] Liang L-L, Chu S-C, Du Z-G, Pan J-S. Surrogate-assisted Phasmatodea population evolution algorithm applied to wireless sensor networks Wirel. Netw. (2022):1-19.
[6] Sandhu RS, Samarati P. Access control: Principle and practice. IEEE Commun Mag 32(9). (1994):40-48.
[7] Benantar M. Access control systems: Security, identity management and trust models: Springer. (2006).
[8] Qihua W, Hongxia J. Data leakage mitigation for discretionary access control in collaboration clouds. Proceedings of the 16th ACM symposium on access control models and technologies. (2011), pp. 103-112.
[9] Sven B, Stephen H, Ahmad-Reza S. Flexible and fine-grained mandatory access control on android for diverse security and privacy policies 22nd {USENIX} security symposium ({USENIX} security 13). (2013), pp. 131-146.
[10] Hongjiao L, Shan W, Xiuxia T, Weimin W, Chaochao S. A survey of extended role-based access control in cloud computing. In: Proceedings of the 4th international conference on computer engineering and networks: Springer. (2015), pp. 821-831.
[11] Liu D, Dong A, Yan B, Yu J. DF-RBAC: Dynamic and fine-grained role-based access control scheme with smart contract. Procedia Comput Sci 187. (2021):359-364.
[12] Hu Vincent C, Richard KD, Ferraiolo David F, Jeffrey V. Attribute-based access control Computer 48(2). (2015):85-88.
[13] Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K. Guide to attribute based access control (ABAC) definition and considerations. NIST Spec Publ 800-162. (2019).
[14] Aghili SF, Sedaghat M, Singelée D, Gupta M-A. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. Future Gener Comput Syst 131. (2022):75-90.
[15] Hao J, Huang C, Ni J, Rong H, Xian M, Shen X. Fine-grained data access control with attribute-hiding policy for cloud-based IoT. Comput Netw 153. (2019):1-10.
[16] Ravidas S, Lekidis A, Paci F, Zannone N. Access control in internet-of-things: A survey. J Netw Comput Appl 144(15). (2019):79-101.
[17] Kayes ASM, Rahayu W, Watters P, Alazab M, Dillon T, Chang E. Achieving security scalability and flexibility using fog-based context-aware access control. Future Gener Comput Syst 107. (2020):307-323.
[18] Aftab MU, Oluwasanmi A, Alharbi A, Sohaib O, Nie X, Qin Z, Ngo ST. Secure and dynamic access control for the Internet of Things (IoT) based traffic system PeerJ Comput. Sci. (2021):1-26.
[19] Bhatt S, Pham TK, Gupta M, Benson J, Park J, Sandhu R. Attribute-based access control for AWS Internet of Things and secure industries of the future. IEEE Access 9. (2021):107200-107223.
[20] Zhang Y, Yutaka M, Sasabe M, Kasahara S. Attribute-based access control for smart cities: A smart-contract-driven framework. IEEE Internet Things J 8(8). (2021):6372-6384.
[21] Lyu Q, Qi Y, Zhang Z, Liu H, Wang Q, Zheng N. SBAC: A secure blockchain-based access control framework for information-centric networking Netw. J Comput Appl 149. (2020):1-17.
[22] Ghaffari F, Bertin E, Crespi N, Behrad S, Hatin J. A novel access control method via smart contracts for internet-based service provisioning. IEEE Access 9. (2021):81253-81273.
[23] Liu Y, Qiu M, Liu J, Liu M. Blockchain-based access control approaches, 8th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud/7th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom. (2021), pp. 127-132.
[24] Carvalho M SE. CaaS-security as a service. Inf Syst. (2011):20-24.
[25] Sharma D, Dhote CA, Potey M. Security-as-a-service from clouds: A comprehensive analysisInt. J Comput Appl 67(3). (2011):1-4.

[26] García-Teodoro P, Camacho J, Maciá-Fernández G, Gómez-Hernández JA, López-Marín VJ. A novel zero-trust network access control scheme based on the security profile of devices and users. Comput Netw 212. (2022):109068.
[27] Rose S, Borchert O, Mitchell S, Connelly S, Zero Trust. Architecture. NIST Spec Publ. (2020):800-207.
[28] Garvis J, Chapman JW, Zero Trust. Security, an enterprise guide A press: Berkeley, CA. (2021).
[29] Aghili SF, Sedaghat M, Singelée D, Gupta M. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. Future Gener Comput Syst 131. (2022):75-90.
[30] Secure Schemes for Secret Sharing and Key Distribution Technion – Israel Institute of Technology: Faculty of Computer Science. (1996).
[31] Dobraunig C, et al. Ascon v1. 2 submission to nist, NIST round, Volume 2. (2019).
[32] Cruz JP, Kaji Y, Yanai N. RBAC-SC: role-based access control using smart contract. IEEE Access 6. (2018):12240-12251.
[33] Guide to attribute based access control (abac) definition and considerations [Draft]. NIST Spec Publ 800(162). (2013):1-54.
[34] Liu D, Dong A, Yan B, Yu J. DF-RBAC: Dynamic and fine-grained role-based access control scheme with smart contract, procedia computer science, Volume 187. (2021), 359-364,ISSN 1877-0509.
[35] Beranger J, Rizoulieres R. The digital revolution in health: John Wiley & Sons. (2021).
[36] Elayan H, Aloqaily M, Guizani M. Digital twin for intelligent context-aware IoT healthcare systems. IEEE Internet Things J 8(23). (2021):16749-16757.
[37] Yadav P, Steinbach M, Kumar V, Simon G. Mining electronic health records (EHRs) a survey. ACM Comput Surv 50(6). (2018):1-40.
[38] Khan WZ, Ahmed E, Hakak S, Yaqoob I, Ahmed A. Edge computing: A survey. Future Gener Comput Syst 97. (2019):219-235.
[39] Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: Vision and challenges. IEEE Internet Things J 3(5). (2016):637-646.
[40] Gupta R, Reebadiya D, Tanwar S. 6G-enabled edge intelligence for ultra -reliable low latency applications: Vision and mission. Comput Stand Interfaces 77. (2021):article 103521.