ISSN 8756-6990, Optoelectronics, Instrumentation and Data Processing, 2024, Vol. 60, No. 2, pp. 297–307. © Allerton Press, Inc., 2024.
ISSN 8756-6990, Optoelectronics, Instrumentation and Data Processing, © 2024, Allerton Press, Inc., 2024.

ARTIFICIAL INTELLIGENCE METHODS

Comparative Analysis of Ontology Based Data Access Control and Security Enhancement in Healthcare Application

Suthan Renuka[1]* and Chirathally Dyamanna Guruprakash[1]

[1] *Department of Computer Science Engineering, Shri Siddhartha Institute of Technology, Maralur, Tumakuru, Karnataka 572105, India*

Received February 26, 2024; revised April 8, 2024; accepted April 17, 2024

Abstract—Formal, machine-readable theories, taxonomy definitions, and connections to human-readable language make up ontology, the formal specification of conceptualization. In addition to methodical definitions, it offers axioms that guide the interpretation of words. Many other sorts of relationships, both structural and nonstructural, including inheritance, generalization, aggregation, and instantiation, are supported by an ontology. It is necessary to handle a number of security issues, including identity management, cryptography, trust, application security, authentication, access control, and privacy. Access control is the process of maintaining resource privacy, project-based group membership, and role specificity in accordance with the goals of the ontology under the proposal. This research examines and contrasts three different ontology-based access control strategies: attribute-based access control (ABAC), context-based access control (CBAC), and role-based access control (RBAC). I-RBAC, BRBAC, SA-ODC and RBACSE are the RBAC approaches used for comparison. For analysing the CBAC procedure, ACAIA, CAHMS, CASPSA and FBCAAC algorithms are used. Finally for evaluating the ABAC method, OABAC, FABAC, AWS-IoTAC and ABAC-PHR algorithms are employed. CASPSA, CAHMS, ACAIA and FBCAAC has a data retrieval time of 1.8, 2.4, 6.1, and 9.4 s. IRBAC, BRBAC, SA-ODC and RBACSE has a turn around time of 66.3, 79.1, 150.5, and 177.2 s respectively. According to the experimental results, attribute based access control systems perform better for securing healthcare data.

DOI: 10.3103/S8756699024700353

Keywords: *healthcare security, ontology, context-based access control (CBAC), role-based access control (RBAC), attribute-based access control (ABAC)*

INTRODUCTION

The development of distributed computing, web services, and service-oriented architecture led to the creation of the innovative technology known as cloud computing. It can provide processing power, data, apps, and other computer infrastructures that are distributed over several sites over a network upon demand [1]. Cloud computing offers a range of scalable, reliable, and services at competitive costs, such as platform as a service (PaaS), software as a service (SaaS), infrastructure as a service (IaaS), and everything as a service (XaaS) [2]. Cloud computing service environments require careful consideration of several security problems, such as identity management, cryptography, trust, authentication, access control, and privacy. Specifically, in cloud computing environments and for integrated administration, an access control and user authentication paradigm is required. and control since different levels of users need to access data [3]. Patient health record digitalization is becoming increasingly important in the healthcare industry since people can now visit hospitals without physically carrying large files including their medical history [4]. Before transferring their PHR data to cloud servers, patients must encrypt it because they forfeit physical control over their health information when PHRs are stored in the cloud [5]. Reducing risks and ensuring company continuity by mitigating the effects of security breaches are the primary goals of the SMS [6].

*E-mail: sutrenuka123@gmail.com

Identification, control of access, management of identities, confidentiality, security of applications, cryptography, and trust are a few security concerns that must be handled in the context of mobile computing services [7]. In particular, because multiple user levels access data in mobile computing contexts, integrated management and control requires a user identification and access control architecture. Before accessing PHRs through mobile applications, patients must encrypt their personal health records because they no longer have physical control over the information [8]. Systems that identify and stop insider intrusions often use the role-based access control (RBAC) and context aware RBAC (C-RBAC) paradigms. However, because RBAC lacks context-aware components, it is unable to offer dynamic access control. Because C-RBAC ignores the degree of security in between, it cannot guarantee the protection of integrity and privacy [9].

The study of items and their relationships is known as ontological theory [10]. This system uses an ontology-based approach, where people and their relationships can be represented to conceptually characterize PHR information in the cloud and to decide PHR access authorization for users, while focusing on PHR access control in dynamic and decentralized users [11]. In an emergency, access control mechanisms that govern and restrict the exposure of data in the healthcare industry are frequently circumvented. The representation and correlation of therapeutic terms is the primary application of ontologies in the medical field. In order to effectively preserve and communicate patient-related material as well as general restorative learning, doctors developed their own unique dictionaries and dialects [12]. Such expressions, sophisticated for human preparation, are illustrated by a great deal of specific knowledge. On the other hand, restorative data frameworks should most definitely clearly convey unexpected and itemized medicinal thoughts. This is obviously a difficult task that necessitates a thorough analysis of the concepts and organization of therapeutic phrasings. Numerous articles are being written to improve security in applications used in healthcare.

COMPARISON OF VARIOUS ONTOLOGY BASED APPROACH

Adoption of internet of medical things (IoMT) solutions is hampered, in part, by concerns about security and privacy. In order to maintain patient data security and confidentiality, IoMT adopters must abide by security and privacy policies. Security toolbox: Context-aware security enhancement in healthcare applications, role-based access control systems, and attacks and countermeasures (STAC).

Role Based Access Control

A role can be thought of as a collection of duties or tasks connected to a certain function inside an organization. Instead of being provided to users directly, all grant authorizations in an RBAC architecture deal with roles. RBAC makes ensuring that particular resources or data are only accessible to those who are authorized.

Intelligent role-based access control (I-RBAC) model. The I-RBAC model, which comprises business and occupational roles and a set of linked tasks, is proposed in the first stage. The proposed I-RBAC model, which incorporates job responsibilities and related tasks, enhances the RBAC model. The utilization of several learning agents and role design that is based on users' official jobs within an organization and given tasks are the key ideas of the I-RBAC architecture [13]. The user (agent), corporate role, task role, task collection, and permission are the primary elements of the proposed I-RBAC paradigm, as illustrated in Fig. 1.

Below are the official definitions of each major component and how they relate to one another in the I-RBAC paradigm.

User agent: A representative is a body that can freely assimilate and interpret changes in its environment and that is aware of its surroundings. It adapts its actions to the changes that have an additional impact on the environment. As a result, the agent is independent and has social skills.

$$Users\left(U_{Ag_i}\right) = \left\{U_{Ag_i}\, i = 1, 2, 3, \ldots n\right\}, \tag{1}$$

where as, $\forall U_{ag} \in U_{Ag}$

$$U_{ag} = \{AID,\ Ontology,\ Communication,\ Action,\ Result\} \tag{2}$$

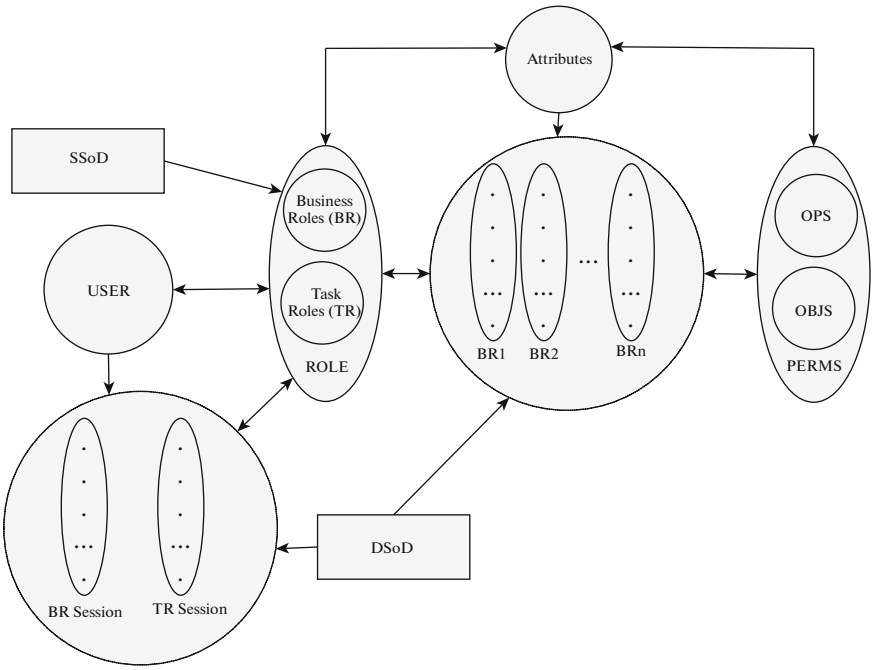

Fig. 1. I-RBAC model.

Role: An organizational title outlining a user's duties. Each user's allocated duties determine which roles they belong in. Known as task roles (TR), task roles are a subset of business roles that are assigned based on their specific tasks. Links between positions and agents are many to many.

$$TR = \{BR_i \; i = 1, 2, 3, \ldots n\}, \tag{3}$$

whereas $\forall br \in TR$

$$br = \{U_{ag1}, U_{ag2}, \ldots U_{agn} \; U_{agi} \in U_{Ag}\}. \tag{4}$$

Blockchain-based role based access control system (BRBACS). The rights of subjects to access resources are represented by role-based access control regulations. This study suggests an auditable, adaptable, and scalable RBAC system built on the EOS blockchain to satisfy enterprise security needs. The EOS blockchain openly records RBAC policies in this suggested method. Administrative positions regulate resources at an elevated level in accordance with how businesses conduct their operations. To control user behavior, an organization establishes roles, role hierarchies, and limitations. This suggested blockchain-based RBAC is compatible with gaseless transactions for delegation capabilities, which makes it palatable and deployable in a wide range of application scenarios. Application agnostic, this suggested method works well for a variety of use situations [14].

Security aware mechanism and ontology based data access control (SA-ODC). The secure awareness technique (SAT) and ontology-based data access control in cloud computing serve as the foundation for this suggested paradigm. The SAT technique was developed to guarantee the security of medical data in cloud computing. It is predicated on encryption, file splitting and adding, and decryption. The goal of the ODAC ontology is to restrict access to data and boost security. Its goal is to build up administrator and owner policies that permit access to data while preventing unauthorised individuals from obtaining data that is being stored. The proposed framework includes a key management mechanism for the SAT approach. The ontology initializes the data control system in order to generate rules that allow the proprietor and operator to provide entry to the information while prohibiting unauthorized users from obtaining the data while it is in storage. This suggested approach is made up of five modules: policy verification, ontology handler, context evaluation engine, control of access engine, and the engine for inference [15].

Role based access control in healthcare information system (RBAC-HIS). Looking for RBAC access control on HIS will provide a variety of results. The reason for this is that, within the context of

HIS, RBAC is quite well-liked and frequently applied. RBAC by itself is impractical; mandatory access control (MAC) and discretionary access control (DAC) must be added in tandem. Added security levels to RBAC that handle the needs for confidentiality or integrity on HIS [16]. In order to increase permission over database tables and rows, the trustworthy health information system (OTHIS) employed a user-centric approach. Additionally, privacy constraints were suggested to be implemented on top of RBAC implementation. This strategy subtly mirrors a recent SBIS mandate.

Context Aware Access Control System

Because different data sources are heterogeneous, retrieving data from multiple sources is more difficult. From the perspective of choosing pertinent data and information gathered from many sources and presenting an integrated data view through information fusion, it is extremely important. For instance, in today's linked contexts, specialists typically only wish to share a portion of their client information, which is typically connected to many data sources. This is true, for example, in applications related to healthcare and defense. Context awareness is introduced by the authors [17]. Context aware systems should have a suitable technique to select the pertinent subset of the application's context information since managing all of the context information is impractical and challenging to complete. Here are some explanations of various context-aware techniques.

Adaptive context-aware IoT (ACAIOT). This suggested framework uses semantic technologies to improve architectural requirements and middleware service requirements. ACAIOT would improve both data and event management for the middleware service needs. It would, however, support the following architectural requirements: abstraction, service-based, semantic interoperability, context awareness, and adaptability. Following are the design ideas that underpin ACAIOT architecture:

- A distinct context management layer that is in charge of producing pertinent context information is used to encapsulate and manage the data and events.
- Supplying a high-level API (ACAIOT Library) to facilitate abstraction requirements by granting access to the backend processing.
- Encourage semantic interoperability to improve the context management process by utilizing ontology and rules.

A context-aware service typically adapts based on the application requirements and context information. Various kinds of context information are gathered from various sources, including sensors, databases, web services, and others, to improve both data and event management. The context management layer, seen in Fig. 2, would assess and interpret all context information. Context-aware services are supplied by this layer to cloud service consumers. ACAIOT, a general-purpose ontology, is expanded into a domain-oriented ontology based on the intended application domain (a smart home domain will be explored in this study). The ACAIOT API and ACAIOT service templates are provided by the next layer, the ACAIOT library. It is important to note that the ACAIOT architecture is broadly applicable across various domains, as it makes it easier to implement cloud services without having to reconsider how to handle such data and events, as well as how to manage and give context information. Figure 2 shows the ACAIOT architecture.

The context manager is used to implement the ACAIOT context management method. The context life cycle phases that were previously described serve as the organizational framework for the primary functional elements of the context management layer. assuming that all data sources registered by the developer using the ACAIOT library are receiving a stream of real-time data as a result of the completion of the context acquisition process. Context modeling, ontology manager, and rule engine are the parts of context manager.

There are four main service kinds that are typically used in context-aware Internet of Things applications: notification, prediction, reminder, and monitoring. These features are supported by the suggested ACAIOT services templates [18]. To meet the needs of his application, the developer modifies ACAIOT services templates. Next, the modified service is implemented using the altered service rules and the context data found in the ACAIOT repository.

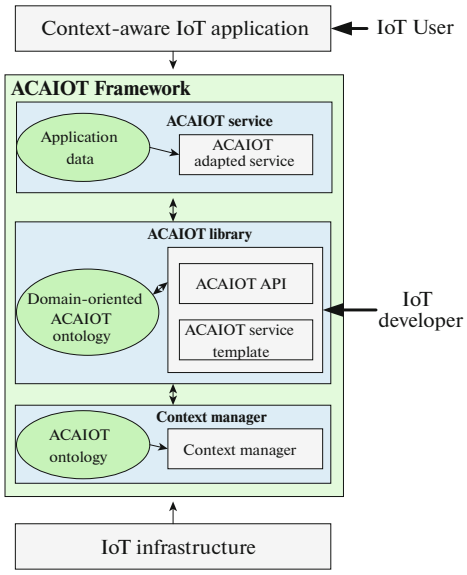

Fig. 2. ACAIOT architecture.

Context aware framework for healthcare monitoring system (CAHMS). The monitored element, which can assume the role of a patient or an elderly or disabled person, is the main component of this paradigm. In order to ensure that decisions are based on a range of observations rather than only the current scenario as given by the current context data, the context history components continuously track the context data of the monitored element. The reasoning engine component uses this data to run the prediction and extract some highly relevant insights regarding the circumstances or health conditions of the monitored element. The monitored element's health or a circumstance that merits consideration is represented by the insight component, such as a fall incidence. The rule engine component receives an insight as soon as it is discovered and uses it to formulate the proper corrective action or actions to remedy the current situation. At the design stage of the HMS process model, the concepts that have been given thus far are subsequently translated onto software components [19]. Additionally, the interactions between these components are developed during this phase, frequently involving the application of a set of design patterns.

Context aware security and privacy as a service in the IoT (CASPSA). Implementing security and privacy mechanisms and managing context awareness separately are necessary to achieve successful context-aware security and privacy. Certainly, greater modularity and flexibility are made possible by the division of intelligence from the implementation of security decisions. Therefore, these capabilities allow for greater flexibility and dynamicness in providing consumers with security and privacy. The knowledge plane (KP) and security and privacy plane (SPP) are thus the two components of the suggested design. In order to offer context awareness, adaptive security, and privacy, these tiers will integrate the ITU-T IoT reference architecture. Integration of the design into new service-oriented networks is made possible by the "as a service" paradigm which tackles many issues related to IoT security [20]. As a result, the virtual network function (VNF) needs are taken into consideration while designing the modules that make up the various planes. IoT application security and privacy will therefore be dynamic, adaptable, user-centric, and flexible.

Fog based context aware access control (FBCAAC). Access control is a crucial security mechanism aimed at preventing unauthorized entry and mitigating the impact of security breaches. An updated version of the fog-based context aware access control (FB-CAAC) platform is provided with the goal of providing adaptable access control information from various sources. This work presents two main contributions to a unique paradigm for context-sensitive access control. One of the main contributions is access control policies, which are designed to reduce processing and administrative overheads when allowing access to various sources of data [21]. Another addition made later on was giving people access to a data view that had all the information they needed from many sources, excluding any combinations of private information that might violate their privacy.

Attribute Based Access Control (ABAC)

The use of ABAC in e-health systems has attracted increasing attention. Concerns about security and privacy are raised when electronic medical records both PHR and HER are shared. ABAC is the strategy that has gained widespread support. Offering granular access to an item or resource depending on the attributes of the subject any entity, including a person, process, or device is the aim of ABAC [22]. As a result, in ABAC, the set of procedures that can be carried out on the object being sought is contingent upon the characteristics of both the subject and the object in question as well as the ambient conditions.

AWS-IoT based access control system (AWS-IoTAC). One essential security measure to protect the Internet of Things is access control. The AWS-IoTAC model includes unique IoT access control elements, such as entities and access control procedures, in addition to the fundamental cloud access control components. It is dependent upon AWSAC, or the AWS cloud access control model. Amazon cloud computing environment. Using accounts, which are basically resource containers, customers may access and control cloud resources as well as manage their invoicing and resource usage. Individuals who have been verified and granted permission to access resources via their accounts are known as Users. An account's owner, known as a user, has the ability to add more users and grant each one of them unique access to cloud resources. User groups make up groups, and the assignment of a user to a group is specified by the user_group relation. Policy-based access control is supported by AWS.

The concept of roles is not the same as the one found in role-based access control. AWS uses roles to provide secure access between various accounts. The Assume role action can be used to create roles with specific permissions that provide access to pertinent cloud resources from multiple accounts. The virtual user role relation specifies the mapping between user roles. Unless otherwise noted, take roles to mean roles for the sake of simplicity. AWS cloud services are referred to as services. In a cloud service like the EC2 virtual machine service, object types designate a specific kind of thing. AWS employs a policy-based access control methodology for access control. AWS policies are established in JSON files that contain permissions set on cloud resources and services. The three primary components (or tags) of it are the following: The virtual user role relation specifies the mapping between user roles. Unless otherwise noted, take roles to mean roles for the sake of simplicity. AWS cloud services are referred to as services. In a cloud service like the EC2 virtual machine service, object types designate a specific kind of thing. When a Principal is associated with a resource, the policy needs to specify the Principal (a user, an account, or a role) it is associated with. Many policies may be associated to one or more entities in order to provide them the required permissions, and one policy may specify multiple permissions.

The related IoT device's identity and most recent known state are preserved by thing shadow. IoT operations (IOP) are a collection of operational activities that are specified for IoT services; they do not include administrative tasks like creating objects, attaching certificates or policies, or creating things. The fundamental set of IoT operations can be divided into a number of categories according to the communication protocols that are used by the devices and apps to link to the AWS IoT service. MQTT clients are capable of four fundamental IoT functions: subscribe, which enables a device to become a member of a particular MQTT topic; connect, which enables a client to establish a connection with the AWS IoT service; and IoT receiver, that enables devices to get information from topics for which they have become subscribers. Comparable methods that HTTP clients can use are IoT update thing shadow, which allows them to send messages to update or alter a thing shadow's state, IoT delete thing shadow, which allows them to remove a thing shadow [23].

Ontology driven attribute based access control (OABAC). The prevalence of cybercrime is on the rise globally, leading to serious security issues that typically discourage small, medium, and big organisations from embracing the cloud paradigm and reaping its many benefits. A method for the semantic modelling of access control policies more specifically, the semantic modelling of the setting of expressions that make up these rules is presented in this work. More precisely, the suggested method enables stakeholders to precisely specify the policies' structure in terms of pertinent knowledge artifacts, allowing them to incorporate their own security and business requirements into these rules [24]. This undoubtedly results in more effective policies while allowing for semantic reasoning regarding policy adherence to the specified structure. The proposed approach provides a reference implementation that extends XACML 3.0 by combining an expert system with reasoning capabilities through suitable meta-rules, thereby mitigating the scalability challenges associated with semantic reasoning.

Formal attribute based access control system (FABAC). According to their attributes, groups are introduced in the suggested model and allocated to various smart entities. Messages, alerts, and adverts from different collaborating smart entities can be accepted or rejected using system-wide regulations. Additionally, it allows the creation of fine-grained security policies and takes into account individual privacy preferences. This section describes an implementation of the proposed ITS-ABAC model utilising AWS IoT services as a proof of concept [25]. These virtual machines submit MQTT messages to an AWS central broker. Additionally, devices using AWS IoT services can be linked together by using a customised endpoint with a REST ARI at each connected device. Devices with clients can publish to and subscribe to reserved, secure topics with the aid of a MQTT broker provided by AWS IoT. As a result, cloud communication is made possible for the clients to interact with any other linked device. In order to implement ABAC regulations specified with the suggested model, Amazon Lambda function has been utilized.

Attribute-based access control in e-health systems (ABAC-PHR). A frequent use case example provides a unified very fine access control mechanism in cloud computing for a specific version of ABAC in PHR. In this approach, the patients kept their encrypted PHRs on a cloud storage platform. A more detailed type of interactive PHR that offers publicly posted composite documents (PPCD), a secure composite document format. Designed for corporate processes, PPCD is a SQLite based serialization that holds many documents with varying formatting and sensitivity. In order to provide simultaneous password-based with private key access, this study suggests a system that brings together the original PPCD-type with an extra new entry table. Password key deduction is the authors' method of protecting privacy and simplifying access revocation. The expanded control over access markup language (XACML) allows for attribute-based access control, which the authors demonstrate may be used to define and protect PHR privacy.

RESULT AND DISCUSSION

The comparison of various ontology based security enhancement approaches in the healthcare system is evaluated and compared in this section. Three different ontology driven techniques such as role based access control, context aware access control and attribute based access control are analysed in this paper. The graphical representation of these comparisons are shown below. The graphs are plotted using Python tool, and the system specifications include an Intel Core i5 CPU, an NVidia GeForce GTX 1650 GPU, a 16-bit operating system, and 16GB of RAM.

Role Based Access Control

The study presents four distinct RBAC methodologies, including the ontology-based data access control (SA-ODC), block chain-based role-based access control system (BRBAC), security aware mechanism, and intelligent role-based access control (I-RBAC) model, role-based access control in healthcare information system (RBACSE).

Comparison of throughput statistic for different algorithms are illustrated in Fig. 3. IRBAC, BRBAC, SA-ODC and RBACSE are the four various algorithms which has a throughput value of 67, 63, 54, and 49, respectively.

Table 1 shows the various statistics analysis of RBAC protocol is given in Table 1. The performances obtained by different algorithms called IRBAC, BRBAC, SA-ODC and RBACSE are low when compared to other current approaches.

Context Aware Access Control System

The performance of various CAAC systems such as adaptive context-aware IoT (ACAIA), context aware framework for healthcare monitoring system (CAHMS), context aware security and privacy as a service in the IoT (CASPSA) and fog based context aware access control (FBCAAC) are compared in this section.

Comparison of received packets statistic for different algorithms are illustrated in Fig. 4. CASPSA, CAHMS, ACAIA and FBCAAC are the four various algorithms which has a received packet value of 94, 87, 83, and 79% respectively.

Table 2 illustrates the performances obtained by various CAAC protocols. These comparison clearly depicts that the CASPSA produce better outcome among the other algorithms such as CAHMS, ACAIA and FBCAAC.

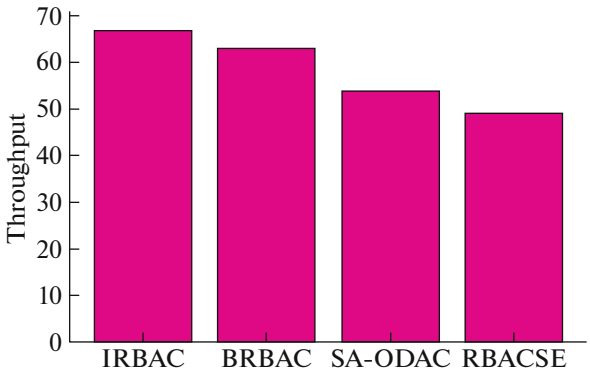

Fig. 3. Examination of throughput statistic.

Attribute Based Access Control (ABAC)

This study compares four alternative approaches: formal attribute-based access control system (FABAC), attribute based access control in e-health systems (ABAC-PHR), ontology driven attribute based access control (OABAC), and Amazon-IoT based access control system (AWS-IoTAC).

Figure 5 shows the ontology processing time metric examination of existing algorithms. It explains how much OPT time produced by each algorithms. 2.1, 4.1, 6.8, and 8.1 s are the ontology processing time produced by OABAC, AWA-IoTAC, FABAC and ABAC-PHR algorithms.

Table 1. Performance evaluation of RBAC protocol

Parameters	IRBAC	BRBAC	SA-ODAC	RBACSE
Data retrieval time, s	0.92	1.7	6.7	10.57
Ontology processing time, s	2.1	5.7	10.1	17.5
Delay, s	3.7	6.9	9.1	13.6
Turn around time, s	66.3	79.1	150.5	177.2

Table 2. CAAC's performance evaluation

Parameters	CASPSA	CAHMS	ACAIA	FBCAAC
Data retrieval time, s	1.8	2.4	6.1	9.4
Received packets, s	2.1	5.7	10.1	17.5
Tardiness, s	5.5	8.2	11.1	15.1
Turn around time, s	56.1	87.1	127.5	173.2

Table 3. Results obtained by various ABAC protocol

Parameters	OABAC	AWA-IoTAC	FABAC	ABAC-PHR
Actual time delay, s	0.9	1.5	3.5	6.2
Throughput, Mbps	62	59	51	48
Delay, s	2.19	5.0	8.1	10.5
Turn around time, s	61.1	73.1	96.5	123.2

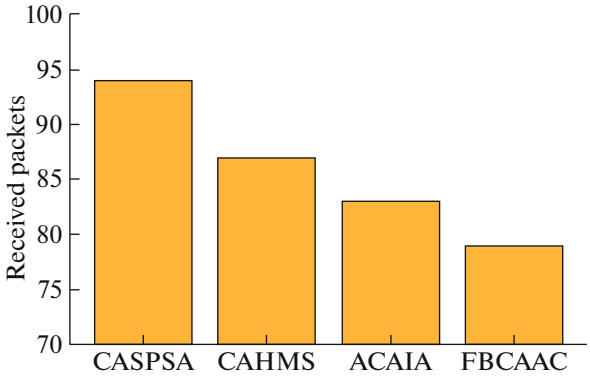

Fig. 4. Examination of received packets.

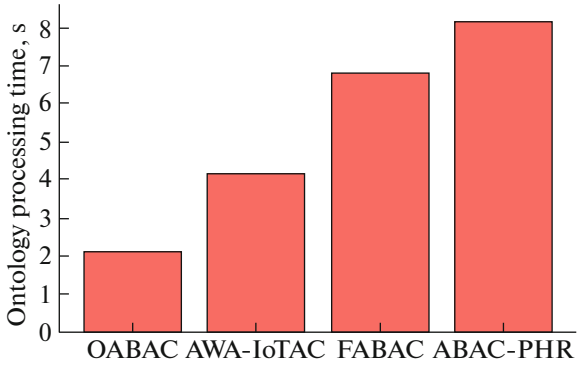

Fig. 5. Comparison of OPT.

Different ABAC protocol's performances are compared and it is given in Table 3. Actual time delay, throughput, delay and TAT are the statistics utilized to compare various protocols named as OABAC, AWA-IoTAC, FABAC, and ABAC-PHR. When comparing all these approaches, OABAC produce better results.

The evaluation of various ontology based data access control approaches called Role Based Access Control, Context Aware Access Control System and Attribute Based Access Control are analysed. It is utilized in different applications such as smart cities, industries and medical field. The efficiency of the compared models are tested using Python and Matlab tools. From these comparisons it is clearly demonstrated that the ontology based data access control approaches produce better outcome for healthcare application.

CONCLUSIONS

This article compares three different ontology based security enhancement technique which are implemented in the test network. The outcomes are compared, and the relevant assessments are done to determine the acceptability of three various approaches. Three techniques have been developed to secure healthcare data: role-based access control, context-aware access control, and attribute-based access control. Algorithms based on roles include the role-based access control (I-RBAC) model, the blockchain-based role-based access control system (BRBAC), the role-based access control in healthcare information system (RBACSE), and security aware mechanism and ontology based data access control (SA-ODC). Adaptive context-aware IoT (ACAIA), context aware framework for healthcare monitoring system (CAHMS), context aware security and privacy as a service in the IoT (CASPSA) and fog based context aware access control (FBCAAC) are the context aware protocols. AWS-IoT based access control system (AWS-IoTAC), ontology driven attribute based access control (OABAC), formal attribute based access control system (FABAC), and attribute based access control in e-health systems (ABAC-PHR) are the attribute based access control protocols. 0.9, 1.5, 3.5, and 6.2 s actual time delay and 2.1, 5.7, 10.1, and 17.5 s of OPT, 66.3, 79.1, 150.5, and 177.2 s of TAT produced by OABAC, AWA-IoTAC, FABAC and ABAC-PHR. CASPSA, CAHMS, ACAIA and FBCAAC has a

data retrieval time of 1.8, 2.4, 6.1, and 9.4 s and Tardiness of 5.5, 8.2, 11.1, and 15.1 s. IRBAC, BRBAC, SA-ODC and RBACSE has a turn around time of 66.3, 79.1, 150.5, and 177.2 s, respectively. The future work is focused on designing a new algorithm to secure healthcare data.

FUNDING

This work was supported by ongoing institutional funding. No additional grants to carry out or direct this particular research were obtained.

CONFLICT OF INTEREST

The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

AUTHOR CONTRIBUTIONS

The corresponding author claims the major contribution of the paper including formulation, analysis, and editing. The co-author provides guidance to verify the analysis result and manuscript editing.

COMPLIANCE WITH ETHICAL STANDARDS

This article is a completely original work of its authors; it has not been published before and will not be sent to other publications until the journal's editorial board decides not to accept it for publication.

REFERENCES

1. A. Nazir, "An ontology based approach for context-aware security in the Internet of Things (IoT)," Int. J. Wireless Microwave Technol. **11** (1), 28–46 (2021). https://doi.org/10.5815/ijwmt.2021.01.04
2. O. Can and D. Yilmazer, "Improving privacy in health care with an ontology-based provenance management system," Expert Syst. **37**, 12427 (2020). https://doi.org/10.1111/exsy.12427
3. S. Karthick, S. P. Sankar, and T. R. Prathab, "An approach for image encryption / decryption based on quaternion fourier transform," in *2018 Int. Conf. on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), Ernakulam, India, 2018* (IEEE, 2018), pp. 1–7. https://doi.org/10.1109/icetietr.2018.8529014
4. S. Kh. Shahzad, D. Ahmed, M. R. Naqvi, M. T. Mushtaq, M. W. Iqbal, and F. Munir, "Ontology driven smart health service integration," Comput. Methods Programs Biomedicine **207**, 106146 (2021). https://doi.org/10.1016/j.cmpb.2021.106146
5. J. Moreira, L. F. Pires, M. Van Sinderen, L. Daniele, and M. Girod-Genet, "SAREF4health: Towards IoT standard-based ontology-driven cardiac e-health systems," Appl. Ontology **15**, 385–410 (2020). https://doi.org/10.3233/ao-200232
6. O. S. J. Nish and S. M. S. Bhanu, "Detection of malicious Android applications using Ontology-based intelligent model in mobile cloud environment," J. Inf. Secur. Appl. **58**, 102751 (2021). https://doi.org/10.1016/j.jisa.2021.102751
7. O. T. Arogundade, A. Abayomi-Alli, and S. Misra, "An ontology-based security risk management model for information systems," Arabian J. Sci. Eng. **45**, 6183–6198 (2020). https://doi.org/10.1007/s13369-020-04524-4
8. N. Sharma, M. Mangla, S. N. Mohanty, D. Gupta, P. Tiwari, M. Shorfuzzaman, and M. Rawashdeh, "A smart ontology-based IoT framework for remote patient monitoring," Biomed. Signal Process. Control **68**, 102717 (2021). https://doi.org/10.1016/j.bspc.2021.102717
9. P. Gonzalez-Gil, A. F. Skarmeta, and J. A. Martinez, "Towards an ontology for IoT context-based security evaluation," in *2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019* (IEEE, 2019), pp. 1–6. https://doi.org/10.1109/giots.2019.8766400
10. N. S. Selvan, S. Vairavasundaram, and L. Ravi, "Fuzzy ontology-based personalized recommendation for internet of medical things with linked open data," J. Intell. Fuzzy Syst. **36**, 4065–4075 (2019). https://doi.org/10.3233/jifs-169967

11. E. Batbaatar and K. H. Ryu, "Ontology-based healthcare named entity recognition from Twitter messages using a recurrent neural network approach," Int. J. Environ. Res. Public Health **16**, 3628 (2019). https://doi.org/10.3390/ijerph16193628
12. S. Singh, S. Ghosh, J. Jayaram, and M. K. Tiwari, "Enhancing supply chain resilience using ontology-based decision support system," Int. J. Comput. Integr. Manuf. **32**, 642–657 (2019). https://doi.org/10.1080/0951192x.2019.1599443
13. R. Ghazal, A. K. Malik, N. Qadeer, B. Raza, A. R. Shahid, and H. Alquhayz, "Intelligent role-based access control model and framework using semantic business roles in multi-domain environments," IEEE Access **8**, 12253–12267 (2020). https://doi.org/10.1109/access.2020.2965333
14. M. U. Rahman, "Scalable role-based access control using the eos blockchain," arXiv Preprint (2020). https://doi.org/10.48550/arXiv.2007.02163
15. G. M. Kiran and N. Nalini, "Enhanced security-aware technique and ontology data access control in cloud computing," Int. J. Commun. Syst. **33**, 4554 (2020). https://doi.org/10.1002/dac.4554
16. M. A. De Carvalho Junior and P. Bandiera-Paiva, "Health information system role-based access control current security trends and challenges," J. Healthcare Eng. **2018**, 6510249 (2018). https://doi.org/10.1155/2018/6510249
17. A. Ghosh, N. Heffernan, and A. S. Lan, "Context-aware attentive knowledge tracing," in *Proc. 26th ACM SIGKDD Int. Conf. on Knowledge Discovery & Data Mining* (ACM, 2020), pp. 2330–2339. https://doi.org/10.1145/3394486.3403282
18. M. Elkady, A. Elkorany, and A. Allam, "ACAIOT: A framework for adaptable context-aware IoT applications," Int. J. Intell. Eng. Syst. **13**, 271–282 (2020). https://doi.org/10.22266/ijies2020.0831.24
19. T. Sylla, M. A. Chalouf, F. Krief, and K. Samaké, "Towards a context-aware security and privacy as a service in the internet of things," in *Information Security Theory and Practice*, Ed. by M. Laurent and T. Giannetsos, Lecture Notes in Computer Science, Vol. 12024 (Springer, Cham, 2019), pp. 240–252. https://doi.org/10.1007/978-3-030-41702-4_15
20. A. S. M. Kayes, W. Rahayu, P. Watters, M. Alazab, T. Dillon, and E. Chang, "Achieving security scalability and flexibility using fog-based context-aware access control," Future Gener. Comput. Syst. **107**, 307–323 (2020). https://doi.org/10.1016/j.future.2020.02.001
21. S. S. L. Chukkapalli, A. Piplai, S. Mittal, M. Gupta, and A. Joshi, "A smart-farming ontology for attribute based access control," in *2020 IEEE 6th Int. Conf. on Big Data Security on Cloud (BigDataSecurity), IEEE Int. Conf. on High Performance and Smart Computing, (HPSC) and IEEE Int. Conf. on Intelligent Data and Security (IDS), Baltimore, Md., 2020* (IEEE, 2020), pp. 29–34. https://doi.org/10.1109/bigdatasecurity-hpsc-ids49724.2020.00017
22. S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-based access control for aws Internet of Things and secure industries of the future," IEEE Access **9**, 107200–107223 (2021). https://doi.org/10.1109/access.2021.3101218
23. S. Veloudis, I. Paraskakis, Ch. Petsos, Ya. Verginadis, I. Patiniotakis, P. Gouvas, and G. Mentzas, "Achieving security-by-design through ontology-driven attribute-based access control in cloud environments," Future Gener. Comput. Syst. **93**, 373–391 (2019). https://doi.org/10.1016/j.future.2018.08.042
24. M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, "An attribute-based access control for cloud enabled industrial smart vehicles," IEEE Trans. Ind. Inf. **17**, 4288–4297 (2020). https://doi.org/10.1109/tii.2020.3022759
25. L. O. Nweke, P. Yeng, S. D., and B. Yang, "Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices," Int. J. Adv. Comput. Sci. Appl. **11** (2) (2020). https://doi.org/10.14569/ijacsa.2020.0110286