Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 01
2024

*Research Article*
https://doi.org/10.56979/801/2024

# A Trust-Driven Optimization of Role-Based Access Control in E-Health Cloud Systems

**Hedi A. Guesmi**[1, *]

[1] Department of Electrical Engineering, College of Engineering, Qassim University, Saudi Arabia
[*]Corresponding Author: Hedi A. Guesmi. Email: h.guesmi@qu.edu.sa

**Received:** September 12, 2024 **Accepted:** November 10, 2024

**Abstract:** In today's world all services related to every sector have made a massive change, especially in health care IT has brought about revolutionary advancement in e-Health. E-Health can only be optimally effective with the integration of Implementing it within a cloud-based infrastructure environment. However, while applying this approach has several benefits, it also raises questions concerning privacy and security. There are inevitable situations when process performance has deteriorated along with the growth of the user base of the Electronic Healthcare Systems (EHS). In response to this challenge, this research presents a novel trust-based access control (AC) mechanism known as Role-Based Access Control (RBAC). It assesses the activity of the user and assigns the position according to the result. The AC module is implemented with SQL server as the back-end administrators may influence user roles and access to EHS several modules. To confirm the trust levels exhibited by users, a.NET-based framework is utilised. The developed new e-Health management framework also confirms the highly secure protection of user data and statistics which are protected against intrusions and other threats.

**Keywords:** E-Health; Role Based Access Control; Trust; Cloud Environment; Data Management

## 1. Introduction

Besides dealing with patients, technology has incorporated numerous complications in managing, storing and exchanging information, device to device, and privacy and security in the healthcare sector. The role of various domains in processing medical data has also added to such complexity. However, cloud computing has come out as the probable solution to these challenges. In the health care sectors, cloud computing improves provider's and consumer's experience through resource provision; services, storage, networks, application and servers. Besides, it also provides security, flexibility and manageability and minimize the potential to lose data [1,2].

healthcare systems are by their nature relational with patient-doctor, pharmacy, and insurance companies being important actors and trust is one of the principal factors that can help in mitigating facets of the healthcare system [3,4]. Now with every field creating an exponential amount of data, there is a requirement of proper and immediate data search. During the real-time search, inter alia, IoT technologies are used, but they need the subject's extensive and intimate data, including location, social contacts, and health status. This is quite a security concern especially if the access control (AC) mechanisms are not effect implemented [5].

HIPAA of 2006 require the security and privacy of patients' health information in the e-records [6]. To meet such requirements, access control is a fundamental enabling technology which strictly controls user's entry to such data under certain circumstances. The most important development in the AC is the Role-Based Access Control (RBAC) of system. RBAC is especially remarkable for its strong securities allowing an administrator, for instance, to create roles that differentiate between a user's authorities [7]. However, permission management in existing AC models is incomplete and lacks effective ways to control permission, as in the folder permission of a computer system. In RBAC administration assigns multiple roles to have permission and control the user's access efficiently.

The different forms of e-Health system are: Patient Portals; Personal Health Records (PHR) A clear difference must also be made between patient portals and personal health records. Of all the applications, patient portals enable people to input data regarding their health status, change family history and even sensitivity information, alongside clinical advice. However, there is a big issue with using the patient data unverified by them and using it unauthorized people [6].

As e-health systems continue to evolve, several challenges remain prominent: 1. Slow System Response Time: An identified crucial weak signal affecting the overall performance of modern e-health systems. 2. Data Security and Permission Management: Making certain data is only available to those with the ability to access it. 3. User Authentication and Monitoring: Authenticating a user and tracking his action to ensure he does not engage in undesired behaviour.

These problems are discussed in the current study, with an emphasis on the utilisation of e-health systems that must, in turn, be capable of implementing original user rights in terms of authorisation and authentication while guaranteeing the efficiency and security of each device.

## 2. Related Work

Ashtiani et al. [4] applied the fuzzy VIKOR technique to analyze trust problems because of its suitability for situation-based problem-solving. This model constitutes a realistic decision-making model especially in access control contexts. Kamesh et al coupled a technique that helped address core challenges to e-health infrastructure. Their concept included a cloud server for data stored and a user-based access control (AC) system together with a central trusted path to extend the trust for AC functions.

Suresh et al. [8] already established an AC model based on resource control through roles and policies of people by increasing the level of security with the help of role bases access control (RBAC) system. The same way, Banyal et al. [9] proposed an AC mechanism that utilized trust control in a cloud environment. When security threats attacked them – whether by accident or on purpose – their security policy built with Linux and NetLogo showed its multi-layered functionality. To overcome the limitation of AC module that do not take into consideration trust relationship between the users and owners, Bhattasali et al. [10] proposed an adaptive AC module. Their system, as checked using Petri Net Designer,is modeled to tackle performance problems by executing phases either offline or online.

In their research, Gupta et al. [11] introduced GCP-IoTAC (Google Cloud Platform Internet of Things Access Control) model stressing on resources and users. The cloud- based e-health system was proposed by Okikiola et al. [12] for using logging-detection and watermarking for the detection of insider attacks. The system they had used was OpenNebula, Microsoft Azure, and MYSQL where their system performance was quite a strong against threats.

The authors of Biswas et al. [13] transformed the existing e-health systems to an integrated blockchain model. Lopes and Gondim [14] proposed a new authentication mechanism for m-health systems for safe and secure direct communication between two devices. The work that is most related to this study is that of Rivera [15] who developed a framework for the formal verification of e-health records where users have control of access. Chiang et al. [16] proposed a framework for creating a digitized patient record that would give authorized doctors full medical background of the patient.

The most recent survey of attribute-based AC in e-health was done by Nweke et al.

[17] and grouped e-health applications pertaining to personal health records. Ashish et al. [18] proposed a secure AC model for cloud-based e-health system using user trust level based approach. Sivan and Ahmad [19] emphasised the increase of cloud solutions applied in e-health, describing security issues. Kanwal et al. [20] studied data privacy in e-health, as well as different privacy and security approaches. Finally, Anilkumar and Subramanian [21] studied the effectiveness of Predicate-Based AC in actual cloud real-time environments like Amazon and Microsoft Azure for fast storage access control.

## 3. Proposed Method

This research introduces several key entities:

### 3.1. Healthcare User (HCU)

A person who wants to find the information about health- care. Healthcare Application: Serves as the channel which the HCU uses to access and request data from the realm of healthcare. Authentication Server: Holder of confir- mation rights with respect to a user's identity and permission to use the application. Trust Evaluation Centre (TEC): Initially used to estimate the reliability of the users. Access Control (AC) Module: Approves and denies access in light of the specific set of access control policies, available resources and the degree of confidentiality of the healthcare information. The proposed trust-based access control module is described in the following Figure 1: User trust levels of users are on a scale of 0 and 1, with 0 representing low or no trust, which means that a user has little confidence in the system, 1 on the other hand represent high trust levels that is a user has full confidence on the system.

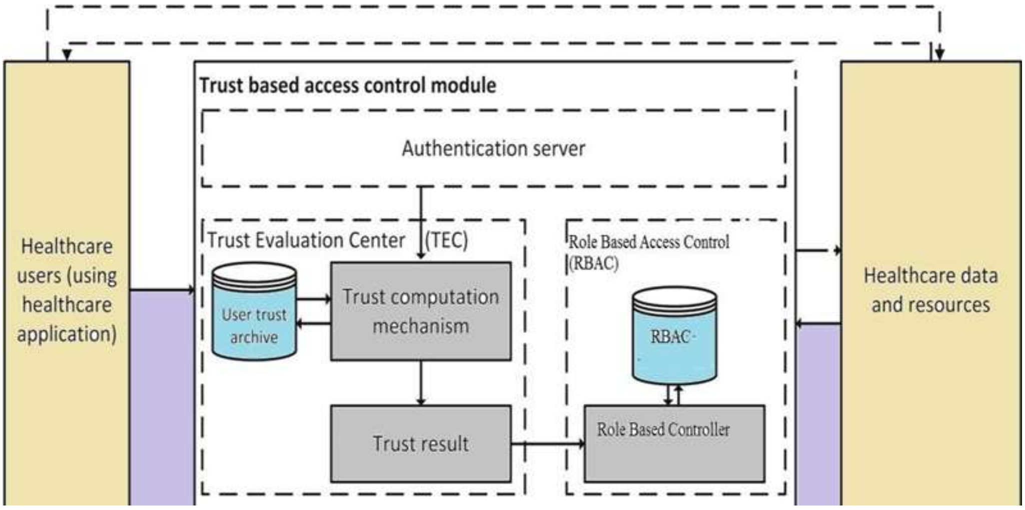
Trust based access control module
Authentication server
Trust Evaluation Center (TEC)
User trust archive
Trust computation mechanism
Trust result
Role Based Access Control (RBAC)
RBAC
Role Based Controller
Healthcare users (using healthcare application)
Healthcare data and resources

**Figure 1.** Proposed trust-based access control module

The proposed framework operates in the following steps:

- **Step 1:** The healthcare user requests access to medical data by providing their credential information (CI) through the healthcare application.
- **Step 2:** The application sends the CI to the authentication server, which checks the validity of the credentials by comparing them with the data stored in its database.
- **Step 3:** If the authentication is successful and access is granted, the Trust Evaluation Centre (TEC) evaluates the user's trustworthiness using predefined trust parameters stored in the user's trust profile.
- **Step 4:** After calculating the trust level, the user's information is sent to the Role-Based Access Control (RBAC) system to process the access request.
- **Step 5:** The RBAC system verifies the user's permissions and decides whether to allow or deny access, based on the trust level and the established access rules

The importance of trust is shown in Fig. 2. Initially, the system verifies the user's credentials. If the credentials are correct, the system proceeds to evaluate the access control and computes the user's trust value. In case the credentials fail authentication, the process returns to Step 1. Once the trust value is computed, access is granted if the trust level is deemed sufficient; otherwise, access is denied. The access control flow is illustrated in Fig. 2.

In Fig. 3, the proposed framework's server role is explained through the following steps:

- The user sends their request to the credential's authentication server.
- After successful authentication, roles are assigned by the server, and the user's information is stored for future reference in the database.
- The user then requests services based on the role assigned by the server to the Policy Enforcement Point (PEP).

- A role-based access request is made using SQL to the Policy Decision Point (PDP).
- The PDP retrieves the policy from its policy repository and gathers the relevant attribute information.
- After collecting the necessary data, the PDP responds to the PEP.
- Finally, access is granted by the RBAC-enhanced web server.

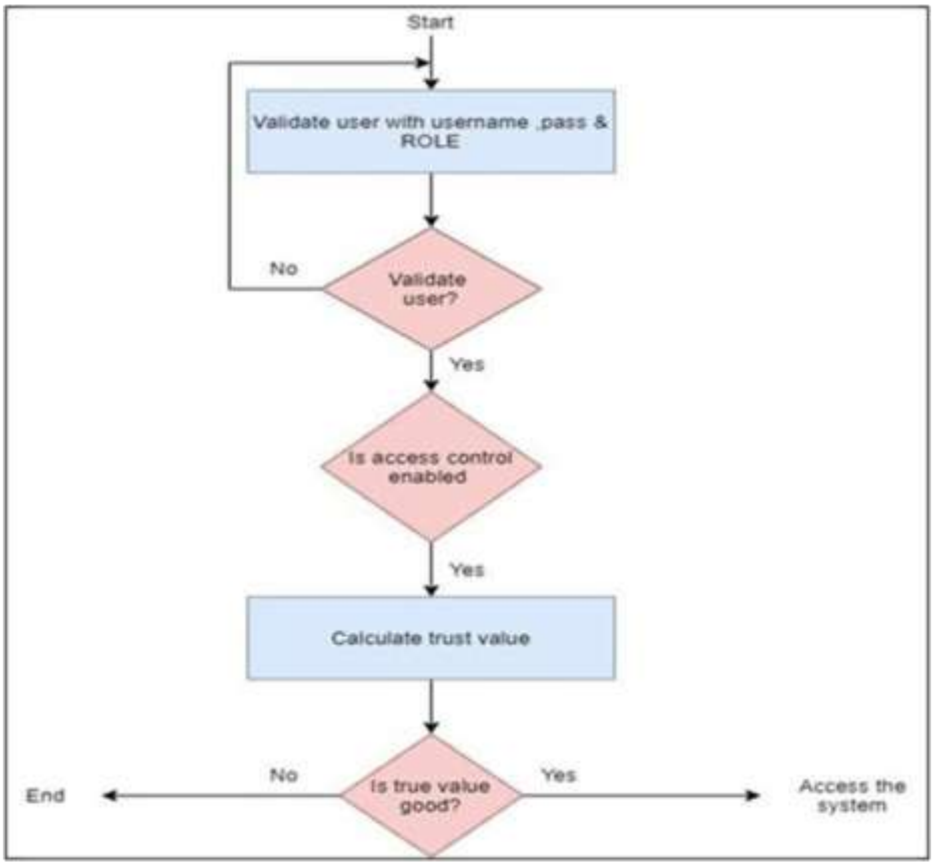

**Figure 2.** Role of Trust

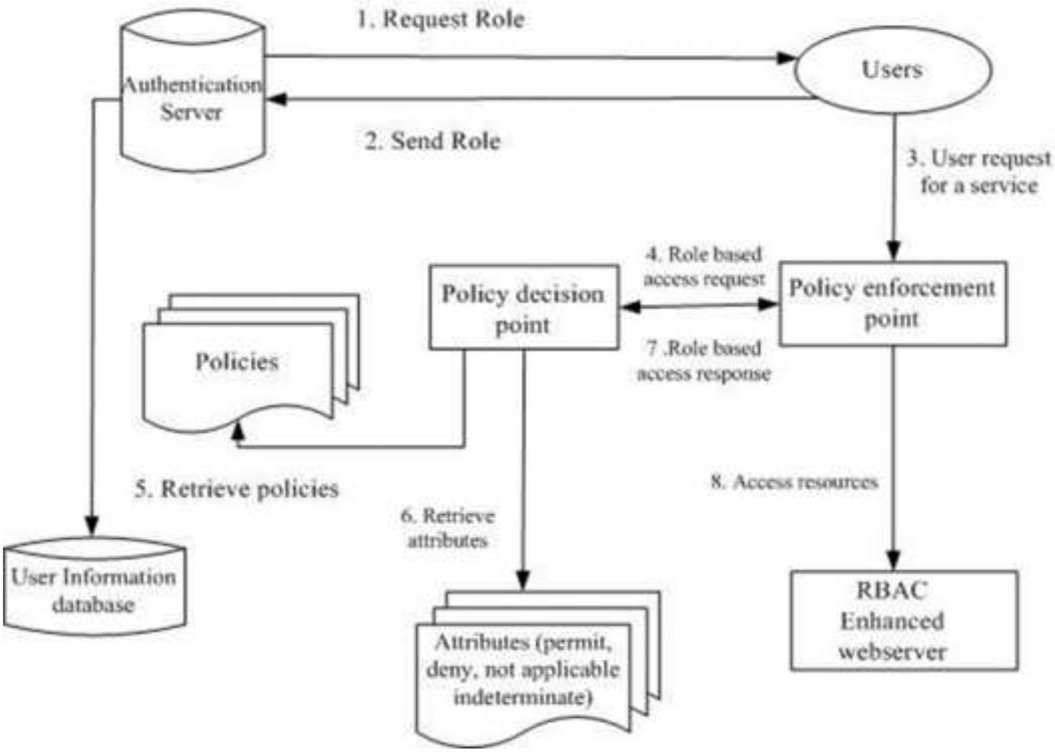

**Figure 3.** Role of Server

## 4. Results and Discussion

The proposed Access Control (AC) module integrates multi-factor authentication along with trust and rTrust mechanisms to enhance security by addressing four critical aspects: user access time, user feedback, performed operations, and environmental conditions. The AC module is implemented using SQL Server. Administrators interact with the system to configure user roles and permissions.

The use of SQL Server ensures secure handling of user data, with access restricted to authenticated users and administrators, providing robust protection. To assess trust values, the system incorporates a C and .NET-based framework. The SQL database stores a history of trust values and user activities, which are tracked according to the four security parameters mentioned earlier. Malicious activities by unauthorized users are logged for future monitoring and analysis.

Thanks to SQL Server's high-performance capabilities, trust calculations are completed quickly, within seconds. Administrators can access audit logs to validate trust values and ensure system security. A trust value between 0 and 0.5 is considered low, while a value between 0.5 and 1 is deemed high. The system calculates the user's trust value during each login attempt, and as the system matures, the Environmental Health Score (EHS) improves.

For example, if the EHS is measured for 100 employees, and there are 20 incidents involving the AC module, but no incidents with the rTrust module, the security level can be calculated using the following equation:

$$1 - {}^{h}\, \frac{AC\ Module\ Cases + 1}{AC\ Module\ Cases + 2}^{\mathrm{k}} \tag{1}$$

1-[20+1/(20+2)]=1-(21/22)=4.54, "hence security is very low."

"Let’s say for EHS of 100 employees, the number of incidents with AC module are say " "20, and number of incidents with rTrust are 130.Then Improvement in security will be in eq.2

$$1 - (rTrustCases) + \frac{1}{(rTrustCases)} + AC\ Module\ Cases + 2 \tag{2}$$

1 - [130+1/(130+20+2)] = 1 - (131/152) = 13.81, "hence the security is improved, rTrust incidents are controlled and employees are aware of security aspects".

Let’s say for EHS of 80 employees, the number of incidents with the AC module is say "20, and the number of incidents with rTrust is 30, then improvement in security will be in eq.3.

$$1 - (rTrustcases) + \frac{1}{(rTrustcases + AC\ \ Module\ \ Cases)} + 2 \tag{3}$$

1-[30+1/ (30+20+2)] = 1-[101/122] = 40.38, "Hence security is improved as employees are aware of unauthorized activities".

The current work focuses on a dynamic access control (AC) module, where the administrator is responsible for managing user access and evaluating the trust levels of all users. The rTrust model is employed to assess user trust. In order to achieve a high level of trust, certain parameters need to ensure that the stored time aligns with the accessed time, such as leave time, on-duty time, and emergency time. The system continuously interacts with the user at different intervals to monitor these conditions. There are two possible scenarios: either the stored time matches the access time (ATmat), or it does not (ATmis). The trust value for the user is calculated based on this assessment, as shown in equation 4.

$$Tat = \frac{ATmat \quad + \quad 1}{ATmat + ATmiss + 2} \tag{4}$$

Where ATmat and ATmis denote the aggregate amount of matched access time and mismatched access time, respectively. The schematic of total access time (Tat) is given in Fig.4.

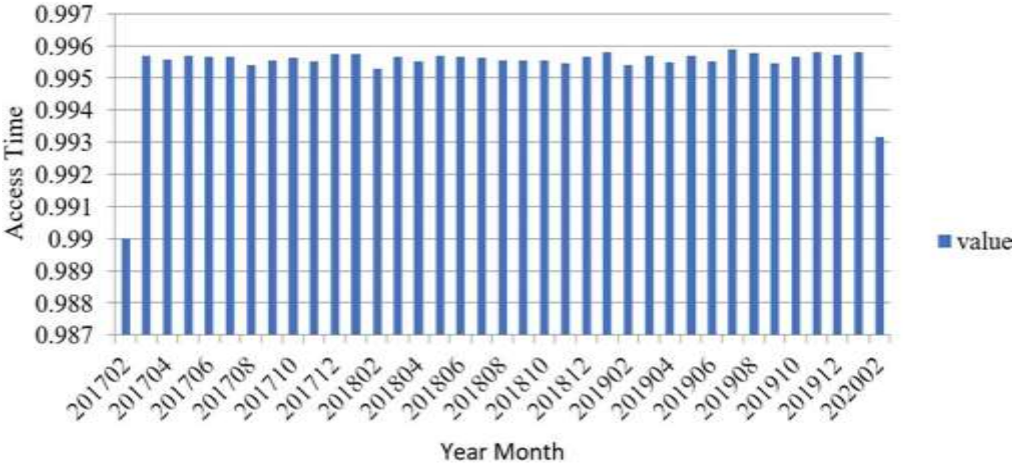

**Figure 4.** Total Access Time of Administrator

User behavior is closely linked to the feedback provided within the system, which can be categorized as either positive or negative. In this context, feedback values range from 0 to 0.5, indicating low feedback, while values between 0.5 and 1 signify high feedback. The trust value associated with the feedback (Tfeed) is calculated as shown in eq.5.

$$T f eed = \frac{FEEDhigh + 1}{FEEDhigh + FEEDlow + 2} \tag{5}$$

Where FEEDhigh and FEEDlow are a collective amount of high feedback and low feedback, respectively. The admin feedback is graphically illustrated in eq.5

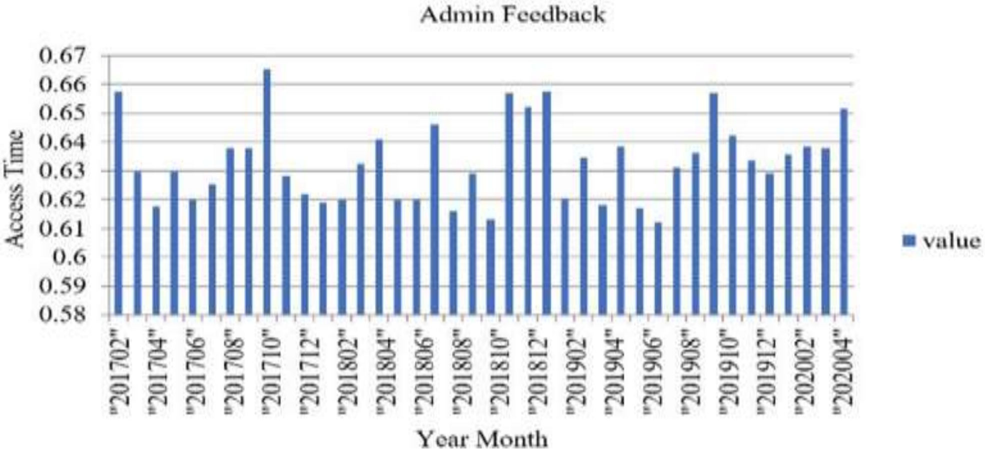

**Figure 5.** Administrator Feedback

In the system, users may occasionally carry out unauthorized actions. The trust value is also determined based on whether the user performs authorized or unauthorized operations. The trust value related to the operations executed (Top) is represented in eq.6.

$$Top = \frac{OP\_auth + 1}{OP\_auth + OP\_unauth + 2} \tag{6}$$

Where OP_auth and OP_unauth are the total number of authorized operations and unauthorized operations, respectively.

The environmental condition is another factor that influences the trust degree and is evaluated during access attempts. If the user logs in or accesses healthcare data from their registered location, their trust degree is considered high, as depicted in Fig. 6. The trust evaluation based on the environmental condition (denoted as Tec) is determined by the following equation (Eq. 7) and is checked in two possible outcomes: True or False.

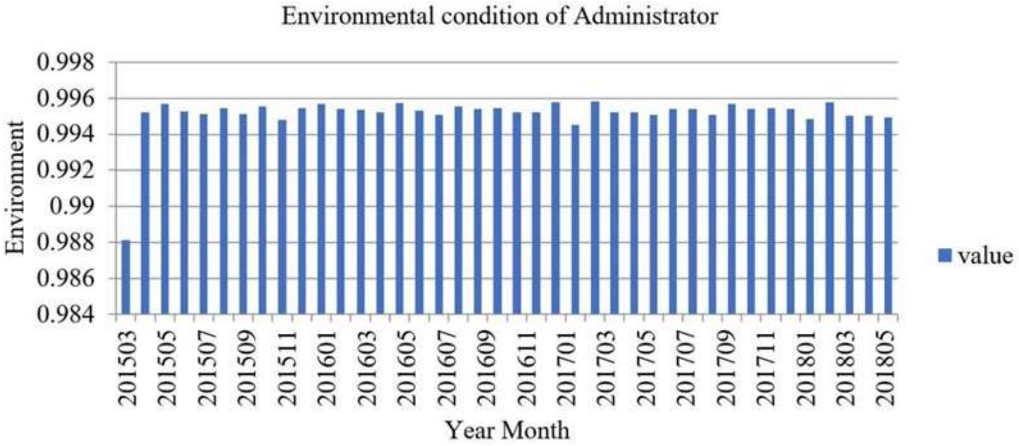

**Figure 6.** Environmental Condition Data Check by Administrator

$$Tec = \frac{EC\_true + 1}{EC\_true + EC\_false + 2} \tag{7}$$

Where EC_true is the total number of times the user accesses the data within the registered location and EC_false is the amount of time, the user accessed the data from an unregistered location.

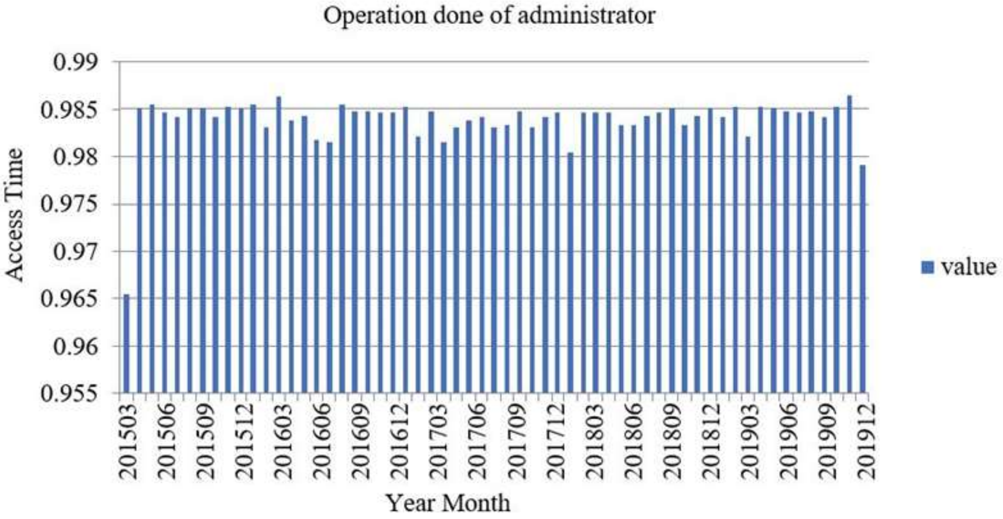

**Figure 7.** Operations Done from Administrator

## 5. Theorem-1

The overall user trust value (Tu-overall) of a requested user 'u' for accessing the data is calculated as follows:

$$\text{Tu-overall} = \alpha 1.UTEP1 + \alpha 2.UTEP2 + \alpha 3.UTEP3 + \alpha k.UTEPn + \alpha 1.Tat + \alpha 2.Tfeed + \alpha 3.Top + \alpha 4.Tec$$

Where $\alpha 1 + \alpha 2 + \alpha 3 + .... + \alpha k = 1$, and $\alpha 1 + \alpha 2 + \alpha 3 + \quad + \alpha k$ are the weights for each UTEP. With Tec Model. The security is improved as the trust value of the user is considered by the AC module to decide the access or deny access to the user. Security has a major concern in every system, here in the below equations eq.8 and eq.9 security is measured with or without trust.

$$1 - \frac{((ACmodulecase) + 1)}{(ACModulecases)} + 2 \tag{8}$$

$$1 - (rTrustCases) + \frac{1}{(rTrustCases)} + ACModulecases + 2 \tag{9}$$

3.1. Parameters Measurements from Administrator

Here graphs are presented of administrator access time in Fig.4, feedback of administrator in Fig.5, environment condition checked by administrator in Fig.6, and operation done from the administrator in Fig.7.

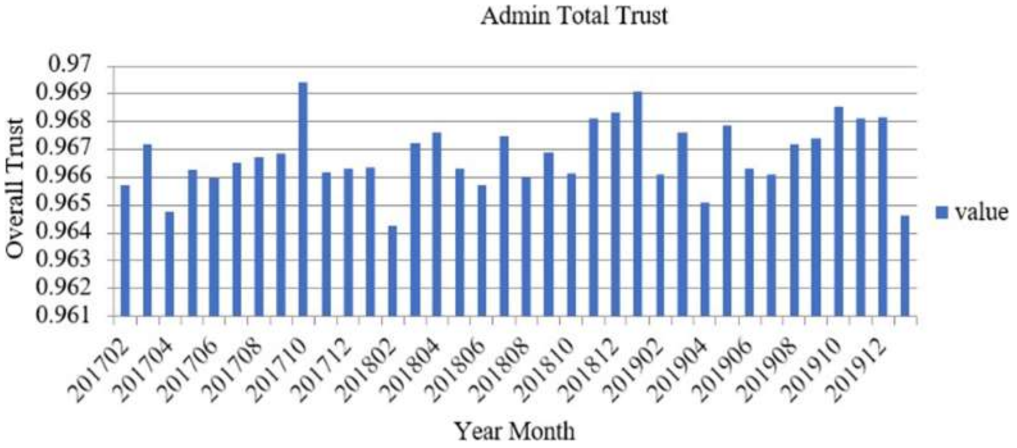

**Figure 8.** The Admin Total Trust

The overall administrator trust and the full confidence of executives are graphically presented in Fig. 8. In this figure, the confidence values range from 0 to 1. To calculate the total trust of the administrator, the following equation and methodology were applied. The administrator checks the condition in Fig. 6, and the operation is carried out as shown in Fig. 7. Fig. 8 illustrates the total trust of the administrator and the complete confidence of the executives. The confidence values are calculated on a scale from 0 to 1. The equation used to determine the total trust of the administrator is as follows:

$$Total\_trust = \alpha 1 Taut + \alpha 2 + T\,feed + \alpha 3 Tec + \alpha 4 Top \tag{10}$$

$$\text{here, } \alpha 1 = 0.3189,\ \alpha 2 = 0.064,\ \alpha 3 = 0.4512,\ \alpha 4 = 0.1657$$

$$\alpha 1 + \alpha 2 + \alpha 3 + \alpha 4 = 1$$

The approach put forward in this study improved the security of the Electronic Healthcare System (EHS) through the combined use of an advanced RBAC Model, with a trust assessment framework. Therefore, the benefit of the methods of the multifactor authentication, the assessment of trust, and the dynamic role assignment is in the drastic increase of the data safety of users and the decrease of possible threats for the system. The client has an effective way through which the specific roles to be assumed by users can be determined from their behavior assessments derived from trust factors, including; time of access, response, operation exerted and environment.

The feature of the adaptation of SQL Server means that with high performance the AC module works with fast rates of data processing within which scales trust value calculations within fraction of a second. Besides, the programing of the trust validation through .NET based framework is not only enhancing the security aspect but also opens up the path to expand the trust model since new parameters and new trust factors can be added in if they are found in the future.

A major strength of this model is that its flexibility can allow for subject- and security-sensitive users to implement the model effectively. For instance, the trust worthiness level keeps on being evaluated and monitored by factors such as user comments and other operational activities, and as a result, roles are dynamically assigned to enable users to gain access only to resources that befit their trust level. This increases security and performance of the EHS system because low trust users will be restricted from sensitive features and data by operations access control.

Nevertheless, it is important to remark that the study has some limitations which are worthy to be studied in the future analysis. This is especially true when as many as 100 users request access and the system starts to slow down a little. While the system expands, especially in the extensive healthcare settings, the I/O response time can slow down thus reducing the efficiency of the system. To counter this, what might be done is to look into the possibility of reducing the time taken by the server to process the queries on the replicative side of the designed SQL Server-based architecture. Moreover, there is a possibility to expand the number of trust parameters, including the actual-time behavioural analysis or the machine learning-based anomaly detection to have more regular and uninterrupted trust estimations. These enhancements would enable the system to achieve better adaptability to the levels of risk for even greater improvement in security.

Further, although the system incorporates the capability of logging suspicious operations to thereafter prevent unauthorized operations, another research frontier can be centered on the discovery of better ways of detecting and preventing malicious operations. For example, predictive modeling and artificial intelligence data could be incorporated and used to project data breaches from the past thereby presenting prevention strategies before the problem occurs.

Hence, the suggested approach gives a good solution for enhancing the EHS system security. Together with using such RBAC-based mechanisms as trust models and dynamic role management, it provides, in fact, an effective solution to protect the processed medical information. However, the following areas are highlighted as potential for further improvement: scalability of the study and an increase in the number of trust parameters that could make the given framework more robust in bigger scenarios.

## 5. Conclusion

Various challenges can arise in different electronic healthcare systems, particularly in securing Environmental Health Score (EHS) data. Protecting this data has become a significant research focus in recent years, with numerous solutions proposed to counter various types of attacks. This study presents a solution based on Role-Based Access Control (RBAC), which is considered more effective than many existing solutions. The research integrates Access Control (AC) modules with trust mechanisms to address the security weaknesses found in current AC systems. In this model, the trust level of a user is incorporated into the RBAC framework, where it is used to monitor user behavior. Users are assigned roles based on their behavior and the trust level assessed. The access control (AC) module is implemented using SQL Server, enabling administrators to oversee access to different parts of the EHS system. Trust validation is carried out through a .NET-based framework, which ensures that customer data is protected from unauthorized access and potential security risks. However, the study acknowledges certain limitations. For example, when over 100 users attempt to access the EHS system concurrently, the system may experience slower response times. Additionally, the trust evaluation could benefit from incorporating more trust parameters to enhance its accuracy.

**Acknowledgments:** The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support [QU-APC-2024-9/1]. Conflicts of Interest: “The authors declare no conflict of interest”.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Azeez, N.A.; Van der Vyver, C. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal 2019, 20, 97–108.
2. Dang, L.M.; Piran, M.; Han, D.; Min, K.; Moon, H.; others. A survey on internet of things and cloud computing for healthcare. Electronics 2019, 8, 768.

3. Ardagna, C.A.; Di Vimercati, S.D.C.; Foresti, S.; Grandison, T.W.; Jajodia, S.; Samarati, P. Access control for smarter healthcare using policy spaces. Computers & Security 2010, 29, 848–858.
4. Ashtiani, M.; Azgomi, M.A. Trust modeling based on a combination of fuzzy analytic hierarchy process and fuzzy VIKOR. Soft Computing 2016, 20, 399–421.
5. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. IEEE Internet of Things Journal 2020, 7, 4682–4696.
6. Kruse, C.S.; Smith, B.; Vanderlinden, H.; Nealand, A. Security techniques for the electronic health records. Journal of medical systems 2017, 41, 1–9.
7. Singh, A.; Chatterjee, K. ITrust: identity and trust based access control model for healthcare system security. Multimedia Tools and Applications 2019, 78, 28309–28330.
8. Suresh, L.; Dash, S.; Panigrahi, B. Artificial intelligence and evolutionary algorithms in engineering systems. Proceedings of ICAEES 2014, 1.
9. Banyal, R.; Jain, V.; Jain, P. Dynamic trust based access control framework for securing multi-cloud environment. Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 2014, pp. 1–8.
10. Bhattasali, T.; Chaki, R.; Chaki, N.; Saeed, K. An adaptation of context and trust aware workflow oriented access control for remote healthcare. International Journal of Software Engineering and Knowledge Engineering 2018, 28, 781–810.
11. Gupta, D.; Bhatt, S.; Gupta, M.; Kayode, O.; Tosun, A.S. Access control model for google cloud iot. 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, 2020, pp. 198–208.
12. Okikiola, F.M.; Mustapha, A.M.; Akinsola, A.F.; Sokunbi, M.A. A new framework for detecting insider attacks in cloud-based E-Health care system. 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS). IEEE, 2020, pp. 1–6.
13. Biswas, S.; Sharif, K.; Li, F.; Latif, Z.; Kanhere, S.S.; Mohanty, S.P. Interoperability and synchronization management of blockchain-based decentralized e-health systems. IEEE Transactions on Engineering Management 2020, 67, 1363–1376.
14. G Lopes, A.P.; Gondim, P.R. Mutual authentication protocol for D2D communications in a cloud-based e-health system. Sensors 2020, 20, 2072.
15. Rivera, V. Formal Verification of Access Control Model for My Health Record System. 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS). IEEE, 2020, pp. 21–30.
16. Chiang, D.L.; Huang, Y.T.; Chen, T.S.; Lai, F.P. Applying time-constraint access control of personal health record in cloud computing. Enterprise Information Systems 2020, 14, 266–281.
17. Nweke, L.O.; Wolthusen, S.D. A Holistic Approach for Enhancing Critical Infrastructure Protection: Research Agenda. The International Conference on Emerging Applications and Technologies for Industry 4.0. Springer, 2020, pp. 220–228.
18. Singh, A.; Chandra, U.; Kumar, S.; Chatterjee, K. A secure access control model for e- health cloud. TENCON 2019-2019 IEEE Region 10 Conference (TENCON). IEEE, 2019, pp. 2329–2334.
19. Sivan, R.; Zukarnain, Z.A. Security and Privacy in Cloud-Based E-Health System. Symmetry 2021, 13, 742.
20. Kanwal, T.; Anjum, A.; Khan, A. Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Cluster Computing 2021, 24, 293–317.
21. Anilkumar, C.; Subramanian, S. A novel predicate based access control scheme for cloud environment using open stack swift storage. Peer-to-Peer Networking and Applications 2021, 14, 2372–2384.