IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment

ATEEQ UR REHMAN BUTT[1], TARIQ MAHMOOD[1,2], TANZILA SABA[1], SAEED OMER BAHAJ[3], FATEN S. ALAMRI[4], MUHAMMAD WASEEM IQBAL[5] AND AMJAD R KHAN[2]

[1]Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh, 11586, Kingdom of Saudi Arabia; ateeqbutt13@live.com, tmsherazi@ue.edu.pk, dramjadkhanu12@gmail.com
[2]Department of Information Science, University of Education, Lahore
[3]Department of Computer Engineering, College of Engineering and Petroleum, Hadhramaut University, Mukalla -50511 Hadhramout, Yemen, saeedalibahaj12@gmail.com
Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, P.O.Box 84428, Riyadh, 11671, Saudi Arabia, fsalamripnu@gmail.com
[5]Department of Software Engineering, Superior University, Lahore 54000, Pakistan, waseem.iqbal@superior.edu.pk

ABSTRACT In today's world, services are improved and advanced in every field of life. Especially in the health sector, information technology (IT) plays a vigorous role in electronic health (e-health). To achieve benefits from e-health, its cloud-based implementation is necessary. With this environment's multiple benefits, privacy and security loopholes exist. As the number of users grows, the Electronic Healthcare System's (EHS) response time becomes slower. This study presented a trust mechanism for access control (AC) known as role-based access control (RBAC) to address this issue. This method observes the user's behavior and assigns roles based on it. The AC module has been implemented using SQL Server, and an administrator develops controls for users with roles and access to multiple EHS modules. To validate the user's trust value, A .net-based framework has been introduced. The framework of e-health proposed in this research ensures that users can protect their data from intruders and other security threats.

INDEX TERMS E-Health; Role-Based Access Control; Trust; Cloud Environment; Data Management; IEEE; Health Issue.

I. INTRODUCTION

IN healthcare, the addition of technology brings multiple challenges like data management, storage of data, data exchange between devices, privacy, and security. Multiple domains are involved in sharing and processing medical data, increasing complexity. The impact of information and communication technology (ICT) advancement on healthcare practices worldwide has been significant. The transition from paper-based medical prescriptions to electronic versions has been widely seen, notably in industrialized countries across the globe [1, 2, 3]. The notion of traditional healthcare has become increasingly focused on virtual healthcare. Incorporating technology into the healthcare sector has given rise to a novel concept known as e-health. In the contemporary world, effective time management has become a must. The practice of seeking medical consultations and enduring lengthy line-ups at healthcare facilities has become outdated. In modern society, the pervasive integration of the internet and technology has led individuals to favor a virtual approach when seeking medical treatment. E-health refers to the practice of conducting online consultations using desktop computers and laptops [4, 5, 6]. The cloud-based e-health system can be tailored to the unique requirements of individual patients. Furthermore, using mobile phones for healthcare purposes is commonly referred to as m-health, primarily intended for the self-management of chronic illnesses. E-health systems have proven to be highly beneficial in managing chronic disease patients requiring continuous monitoring. E-health systems are designed to monitor health-related data and offer assistance in several areas, such as symptom assessment, physician selection, financial management, self-monitoring, and prescription fulfillment. The data above is readily available and accessible to a substantial demographic [4, 7].

A. E-HEALTH EMERGENCE & CLOUD-BASED SYSTEMS

The integration of e-health into the healthcare system has emerged as an indispensable component, owing to its efficacy in delivering services and generating precise outcomes while

minimizing errors, in contrast to conventional healthcare systems. In the traditional treatment approach, patients may inadvertently receive duplicate doses of medication due to manual record-keeping procedures. In healthcare, electronic medical records play a crucial role in storing comprehensive patient treatment and drug information, thereby mitigating the risk of medication errors [8]. The success of e-health in a country is contingent upon several aspects, including the type of management and infrastructure employed, the level of user engagement, and the system's scalability to accommodate a wide range of users. The medical data stored in cloud-based systems holds significant value for healthcare experts, consumers, entrepreneurs, and businesses involved in health insurance and related policies. To properly utilize cloud technology in healthcare, it is essential to establish e-health strategies encompassing conventions, legislation, and regulations. The phenomenon under consideration is more than a mere advancement within the realm of technology; rather, it embodies a cognitive framework and mindset aimed at expanding the scope of healthcare. This expansion is achieved by utilizing information and communication technology (ICT), thereby enhancing local, regional, and worldwide healthcare provisions. The term "e-health" refers to the use of electronic devices, such as mobile phones or laptops, in conjunction with cloud technology to store health-related information.

There are two primary categories of eHealth: personal health records (P-HR) and electronic health records (E-HR). Patients utilize the Personal Health Record (P_HR) to independently update their health records and engage in online consultations via mobile devices. While electronic human resources (E-HR) can benefit healthcare workers, The utilization of electronic health records (E-HR) offers significant advantages in delivering appropriate patient care and facilitating the secure exchange of medical records, patient medical histories, medication details, and prescriptions. E-health provides a proficient and immediate therapeutic approach for patients [9]. The necessity to unify and include diverse electronic health data from several sectors, including medical research laboratories, hospitals, and health insurance companies, has given rise to the emergence of an electronic health (e-health) concept. In essence, e-health can be characterized as using IT infrastructure and e-commerce methodologies to facilitate the processing, exchange, and manipulation of health information. It is essential to acknowledge that the involvement of several domains in sharing medical data has presented challenges in managing the application effectively. Therefore, there is a necessity for a cloud-based environment that facilitates the collaborative sharing of information across multiple administrative domains [10, 11]. Cloud computing has numerous advantages, one of which is the efficient and fast transfer and sharing of medical information without any disruptions. Furthermore, this development has alleviated the burden on healthcare providers regarding managing infrastructure and has afforded them numerous opportunities to become acquainted with IT service providers [12, 13]. Cloud computing has been extensively studied in academic literature, where it has been consistently recognized for its various advantages. These advantages include scalability, cost-effectiveness, and the capacity to boost agility and facilitate collaborative resource sharing. It's possible to find the solution to these challenges through cloud computing. In the healthcare sector, cloud computing provides efficient services to healthcare professionals and provides a good patient experience [1]. Cloud computing provides on-demand resources to its users, like services, storage, network applications, and servers. It's also providing security, mobility, and scalability. It also reduces the risk of missing data [14]. Systems in healthcare provision relate to relations between patients, doctors, pharmacies, and insurance companies [15, 16]. Trust is an essential factor in multiple applications and various fields. It is a tool used for decreasing complexity [17]. The amount of data is increasing day by day. To find accurate and quick information, the Internet of Things (IoT) search technology is used to achieve the needs of real-time search. This search also required personal data in large amounts, like information on location, social relations, and personal health [18]. This will cause serious security issues when employing personal information if an active access control (AC) mechanism is missed during the search. Fortunately, the notion of data storage in EHRs has addressed several security problems that have been a barrier to the widespread adoption of cloud-based e-health applications [19, 20, 21]. This is in addition to the benefits that have been listed above. However, the safe and confidential exchange of medical information between patients and healthcare professionals is still difficult and time-consuming. Illegitimate organizations get their hands on clever ways to access electronic health records (EHRs) without having formal authority to do so, which leads to breaches in sensitive data and confidentiality as well as security assaults on e-health platforms [19]. In addition, it can be challenging for patients to keep track of and manage their medical data when it is stored on the cloud and shared with several service providers. Consequently, it is of the utmost importance to propose efficient access control solutions for platforms that share cloud-based EHRs.

B. SECURITY, TRUST MECHANISMS, & ACCESS CONTROL IN E-HEALTH

Conventional ways to access and manage [22, 23] the sharing of electronic health records (EHRs) assume that requesters of cloud computing services are trustworthy, and they permit cloud services to carry out all security controls and authorization obligations linked to data consumption. Unfortunately, this assumption does not hold true for portable clouds because portable clouds feature cloud servers that are honest and inquisitive. Because traditional authentication solutions primarily depend on a specified entry point, sometimes known as a centralized cloud server, e-health connections can potentially have a critical reliance on a single point of failure if this dependency is not managed correctly. According to the Health-Insurance- Portability and

Accountability Act (HIPAA) 2006 in the USA, health information security and privacy are included in the e-records of patients [24, 25]. A technology working as a backbone is AC to certify information security. The AC mechanism monitors access events effectively and certifies that only authorized users get information under authentic conditions. Extensive and advanced development in the AC field is the RBAC scheme. The main attraction of RBAC is based on fully advanced security with a role concept. In RBAC, roles distinguish the user's authorization [26]. Access control is a fundamental method employed in cloud computing environments to ensure the cloud environment's security. The conventional approach to access control primarily consists of an access control model and a policy description language. The primary access control methods commonly employed in various systems are discretionary access control (DAC), mandatory access control (MAC), and RBAC [27]. These three models demonstrate superior performance in a static setting. The dynamic nature of the business environment in cloud computing necessitates careful consideration of the security and integrity of resource access. Relying solely on static rule-based decision-making can pose significant security threats to the system.

The classic token-based technique can be classified as a static access control mechanism. Once the user successfully completes the system's identity authentication process, the system proceeds to allocate a token to the user. Each token serves as a distinct identifier for a user, eliminating the need for the system to authenticate the user in subsequent operations. In the computing environment, it is common practice for the access topic to be situated in a manner that facilitates the caching of the authentication token, thereby enhancing the efficiency of the authentication process. Nevertheless, this strategy presents a notable security concern. One potential consequence of a decline in the security of the primary environment is the potential for unauthorized use of the authentication token, leading to the illicit utilization of system resources and services. Conversely, in situations where the system is operating under emergency conditions, such as when CPU and memory utilization is at maximum capacity, conventional access control mechanisms may continue to grant access requests as long as they are deemed legitimate, thereby heightening the likelihood of a system failure [28, 29]. From the best of the author's information and literature, it could be seen models of AC didn't offer a mechanism for managing permissions. The concept is quite similar to folder permissions in computer systems. This is similar to RBAC, where the administrator creates multiple roles to manage permissions. The two things are different, i.e., the patient's portal and Personal- Health records (PHR). Patients can modify his/her data, intimate lineage, sensitivity, and a blend of clinical advice. In the health system, this area is not too much. People don't hesitate to use patients' information without verifying that this information has not been verified by the clinical master [24] As the e-health system improves daily, some issues are associated with it. In this study, some of them are discussed. Firstly, the system response time is prolonged; secondly, the critical issue is data security and allowing permissions to actual persons; thirdly, user identification and monitoring of users' behavior. How does the system authorize and authenticate the originally requested individual?

C. RBAC IN E-HEALTH: A PROPOSED TRUST MECHANISM

The study introduces a trust mechanism for RBAC in Electronic Healthcare Systems (EHS) implemented in a cloud environment. This mechanism observes and responds to user behavior, assigning roles based on observed behavior. Using SQL Server, the Access Control (AC) module is developed, allowing administrators to set functions and control access to various modules of the EHS. To validate the trustworthiness of a user, a .net-based framework is employed. This proposed e-health framework aims to protect user data against external threats and unauthorized access, addressing the challenges of prolonged system response time, data security, and authentic user identification and behavior monitoring.

Towards this end, our proposed work's major contributions are:

- This study introduces an innovative trust mechanism for e-health, integrating RBAC and behavioral analytics to enhance user authorization paradigms.
- It presents a refined access control paradigm, addressing limitations in granular permission management.
- The study focuses on optimizing system responsiveness, developing a robust data security framework, offering a sophisticated user authentication mechanism, and deploying a Trustworthiness Quantification methodology using a.net base framework for evaluating user trust indices.
- The study addresses the challenges of lagging system responses in e-health infrastructures.

An examination of related research, shortcomings in conventional methods, and the driving force behind the research is presented in Section II. The proposed algorithms are delineated in Section III. The performance of the suggested approach and the ensuing experimental results, evaluated using diverse performance metrics, are deliberated upon in Section IV. Section V expounds upon the accomplishments of the proposed studies, constraints encountered, and avenues for future exploration. Finally, the findings of the research are summarized in Section VI.

II. RELATED WORK

Ashtiani et al. [17] used a fuzzy VIKOR approach for resolving trust issues due to its ability to solve problems according to the situation. This model can also be used alternatively to the approach used in this study due to its decision-making ability. Kamesh et al. [30] proposed to resolve significant issues in the e-health infrastructure. They proposed a hybrid technique to access data from a cloud server and applied a

user-based AC control system; a centralized control system relies on a trust extension mechanism to gain robust and tough AC. Suresh et al.[31] proposed an AC mechanism to limit resource access to enhance security. This system defines roles and policies for each individual separately. The data becomes safer on the cloud because they use the RBAC mechanism. Banyal et al. [32] proposed an AC mechanism with trust control in the cloud environment. They provide the policy of the AC mechanism and add different layers of security. The framework presented in this study was developed on Linux in NetLogo and established with test cases. The results showed that the proposed mechanism was robust and effective against multiple security threats. Bhattasali et al. [33] adopted the AC module, considering the trust association between users and owners. To avoid low performance, phases were executed either offline or online. The proposed framework used Petri Net Designer for verification and formal analysis. A risk-based access control approach was presented by Dos Santos et al. [34], which included the introduction of three new modules: the Risk Engine, the Risk Quantification Service, and the Risk Policy. This method allows users and cloud service providers to determine how to manage problematic access requests, although the research does not disclose precise risk quantification approaches.

An access control model based on fuzzy reasoning was proposed by Li et al., [35]. This model was proposed in terms of the assessment of risk. A predetermined rule is proposed to decide whether to authorize it by analyzing the authorization risk. However, the model does not consider the impact of the user's previous behavior on the risk. This is necessary to realize risk control based on binary linear programming (BLP). They also suggested a fuzzy multi-level access control model to assess the risk of access and dynamically control the flow of risk information by the system's present environment, the business's requirements, and the risk tolerance level. This method takes as inputs the sensitivity of the data, the risk of doctors' behavior, and the historical risk. It then combines historical data and fuzzy sets to assess the medical data access risk level. However, this approach is limited to medical data and is not applicable in other contexts. They developed another classification-based method for risk access control, and this strategy involves classifying risk with authorization and integrating an access control matrix with role-based access control to award permissions to the roles that provide the least amount of danger. Atlam et al., [36] recently proposed using a neuro-fuzzy system model to estimate the value of the security risk that is associated with each access request for various Internet of Things applications. The results of the trials demonstrated that the proposed method provides access decisions that are dynamic and aware of the context in which they are being made based on real-time information. Atlam et al., [37] give a systematically conducted literature review on the various approaches to dynamic access control. Along with the risks associated with access control procedures, the risk assessment approaches and the risk factors utilized to construct them are extracted and assessed. Kesarwani et al., [38] have developed a few ideas for fuzzy trust-based access management. In these methods, trust values have been determined using a variety of factors, including the total number of requests, faulty requests, fraudulent requests, and unlawful requests, as well as the overall number of requests.

A mutual trust-based access control approach that incorporates trust management is proposed by Lin et al. [39]. This model considers both the cloud service provider's reliability and the end users' actions. The cloud's access control and security challenges can be resolved using mutual trust mechanisms between users and the cloud. The idea of trust in role-based access control is proposed by Chunge et al. [40] as a means to detect dangerous users and keep the cloud and data safe. Wu et al. [41] examined various traditional access control methods and proposed a hybrid approach based on role-based access with additional layers of security. The results of the studies showed that the proposed method could improve the system's credibility, reduce the possibility of task failure and spoofing, and prevent unauthorized users from gaining access to sensitive data. A context-aware access control paradigm, as developed by Satoh et al. [42], integrates role- and subject-based frameworks. In this work, we only present the framework's central idea and a working prototype of it.

Gupta et al. [43] proposed a GCP-IoTAC (Google Cloud Platform Internet of Things Access Control) model. Services and their documentation are available in large numbers on GCP. This work focuses on AC and the authorization of resources and users. Okikiola et al. [44] proposed a system using a logging-detection procedure and watermarking extraction to detect insider attacks in an e-health cloud-based environment. This system was implemented by using Opennebula (cloud management software) Microsoft Azure, PHP, and a database server (MySQL). By using this approach, good performance was shown in the results. Biswas et al. [45] migrated a formal e-health system to a single, uniformly managed blockchain-based ecosystem. Gondim et al. [46] proposed a new protocol of authentication in a mobile-health (m-health) system that supports communication between devices and ensures safety.

Rivera et al. [47] proposed a system of formally verifying e-health records regarding how users can access and control their information and how the system manages their access. Chiang et al. [48] proposed a system that digitalized patients' records to facilitate the doctor's checking of the patient's complete medical history. The proposed system ensured security by authorizing only medical personnel to collect information after getting a decryption key for an authorized time slot. Nweke et al. [49] conducted a detailed survey to understand some attributes-based AC applications in e-health. This survey categorizes work according to existing applications, e-health records, personal health (p-health) records, and attribute-based AC. Ashish et al. [50] proposed a secure AC model for e-health in the cloud environment. This model calculates the user's trust level in their behavior. Users' access views are adjusted based on this computed trust

degree. Ahmad et al. [51] focuses on the day-to-day enhanced demand for cloud computing and how these technologies are widely used in e-health. Kanwal et al. [52] researched in detail the privacy of data publicly released in e-health. Why is the privacy of e-health data needed? A detailed comparative analysis of security and privacy techniques is discussed in this study. Anilkumar et al. [53] proposed work that was evaluated and checked in a real-time cloud environment on Amazon Cloud, open-stack Cloud, and Microsoft Azure Cloud. The technique of Predicate-Based AC was proposed to achieve AC for swift storage.

III. RESEARCH FRAMEWORK

A sophisticated trust mechanism is implemented and serves as a critical component in safeguarding the security and dependability of our e-health cloud system. The trust mechanism is an intricately planned computational framework that is responsible for assessing and allocating trust levels to entities and users who are actively participating in the system. An ongoing and vigilant surveillance of user behavior that draws conclusions from both historical data and current behavior distinguishes the system's operation. Through the meticulous application of sophisticated algorithms and predefined trust thresholds, it evaluates the credibility of users. This evaluation takes into account a multitude of elements, such as the frequency of system access, the characteristics of actions executed, and the user's prior engagements with the system.

The seamless integration of this trust mechanism into our comprehensive RBAC system distinguishes our methodology. This integration influences access decisions through the establishment of a dynamic and adaptable access control environment based on levels of trust. The trust scores of users are dynamically recalculated during their interactions with the system, enabling prompt modifications to access privileges. By distinguishing between reliable and unreliable users, this dynamic strategy not only improves security but also contributes to an exceptional user experience. Authorized users are granted priority access, whereas individuals with lower trust scores are subject to more stringent access restrictions. Additionally, a resilient architecture that includes users, roles, and permissions distinguishes our RBAC system. Defined with great attention to detail, roles in the healthcare ecosystem correspond to a wide array of responsibilities. These responsibilities span from those of a "physician" and "nurse" to those of an "administrator" and "patient." The assessment of user behavior by the trust mechanism is intricately connected to the designation of roles. In addition, authorizations are methodically organized in order to govern the entry of healthcare information and essential system operations. By doing so, it guarantees that users are restricted to accessing only those resources and features that are directly pertinent to their designated roles and obligations.

To discourage unauthorized access attempts, our system's security is fortified with a number of measures, including rigorous authentication and authorization protocols. Furthermore, the RBAC system rigorously adheres to the principle of least privilege, ensuring that users are exclusively granted access to the information and functionalities that are fundamental to their designated roles. By implementing this comprehensive strategy, we reaffirm our dedication to protecting the privacy of patients, preserving the integrity of data, and fortifying the e-health cloud system as a whole.

The proposed framework centralizes healthcare data management by intertwining several entities: the Healthcare User (HCU), a dedicated Healthcare Application, an Authentication Server, and the unique Trust-Evaluation Centre (TEC). While HCUs initiate requests for data, these are processed via the Healthcare Application and vetted through the Authentication Server. The TEC, a pioneering addition, rates users based on past interactions, enhancing data security. Decisions on granting access lie with the Access Control (AC) Module, which uses set criteria to determine permissions. Seamlessly integrating these components, the framework is tailored to maintain data sanctity, foster user trust, and balance between ease of access and rigorous safeguarding measures. In Figure 1, a proposed trust-based access control module is presented. For the requested user's trust level, the threshold values differ from 0 to 1, whereas 0 specifies no faith or low confidence, and 1 specifies a good level of trust.

Here, some working of Figure 1 discussed the step-by-step working of the proposed AC module is presented below.

- For the use of medical data, the healthcare server received a request from a healthcare user for credential-information (CI) via the healthcare application
- After passing CI to the authentication server for checking, it checks CI in its stored database.
- When the server checks CI and access is granted, the Trust Evaluation-center (TEC) receives a request and checks the user's degree of trust using parameters stored in the user trust archive.
- After calculating the trust degree, user information is moved to Role-based AC for controlling access
- After receiving user information, the Role-based AC mechanism checks for permissions whether the access is granted or denied

In Figure 2, the role of trust is discussed. Firstly, the system authenticates user credentials. If the credentials are correct, the system checks for access control and calculates the trust value of the user. The system will move on to the first stage if the credentials are incorrect. After calculating the trust value, if the trust value is good, the access for the system is yes or if the trust value is low, then no access will be given. The flow diagram of the access role is provided below in Figure 2. In Figure 3, the sub-part of the proposed work and the role of the server is explained in a few steps.

- After the authentication form, server roles are assigned, and information about the user is stored in the database for future records.
- Services are requested from the user side based on the role allocated from the server to PEP (Policy enforce-

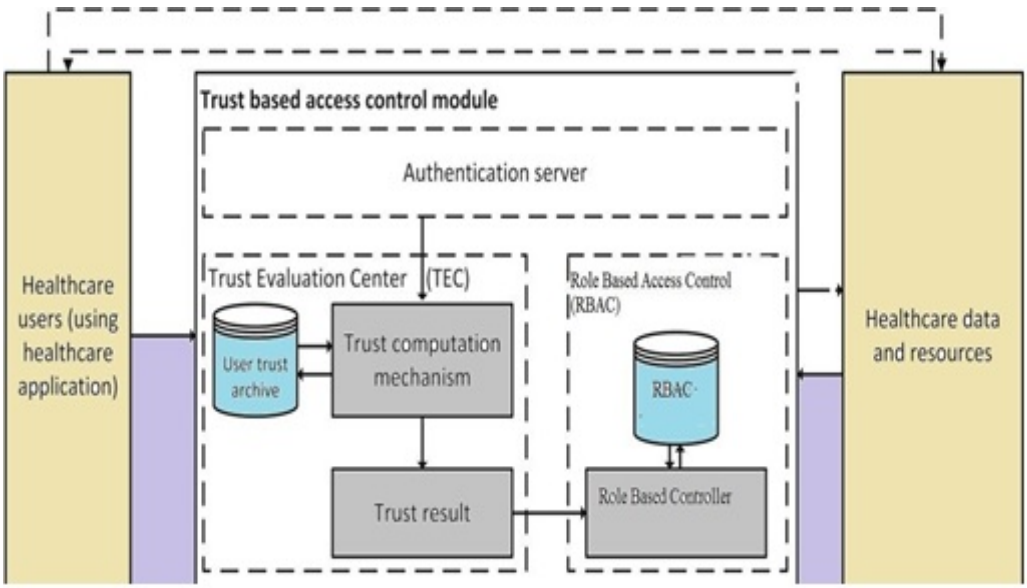

Figure 1: Proposed trust-based access control module

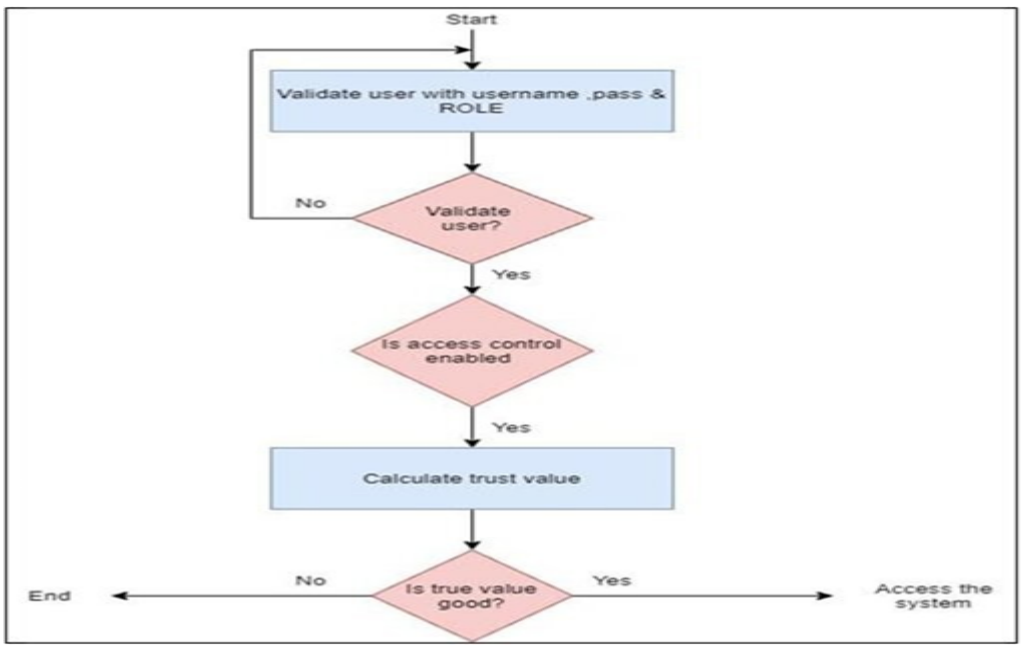

Figure 2: Role of Trust

ment point)

- Role-based access requested using SQL to policy decision point (PDP).
- Here PDP repossesss policy from the repository of policy and then collects relative attribute information.
- After collecting the required information, PDP will respond to PEP.
- Finally, access was allocated to RBAC enhanced webserver.

IV. RESULTS ANALYSIS

By using multifactor authentication, trust, and $rTrust$, the proposed AC module moved towards implementing four aspects of security, i.e., user access time, feedback from the user, operation done, and environmental conditions. SQL Server was used in the implementation of the AC module. Administrators make the approach towards the AC module and generate roles. The implementation of the current work is based on SQL Server. Due to the password protection of the SQL server, information is secured inside and only accessible

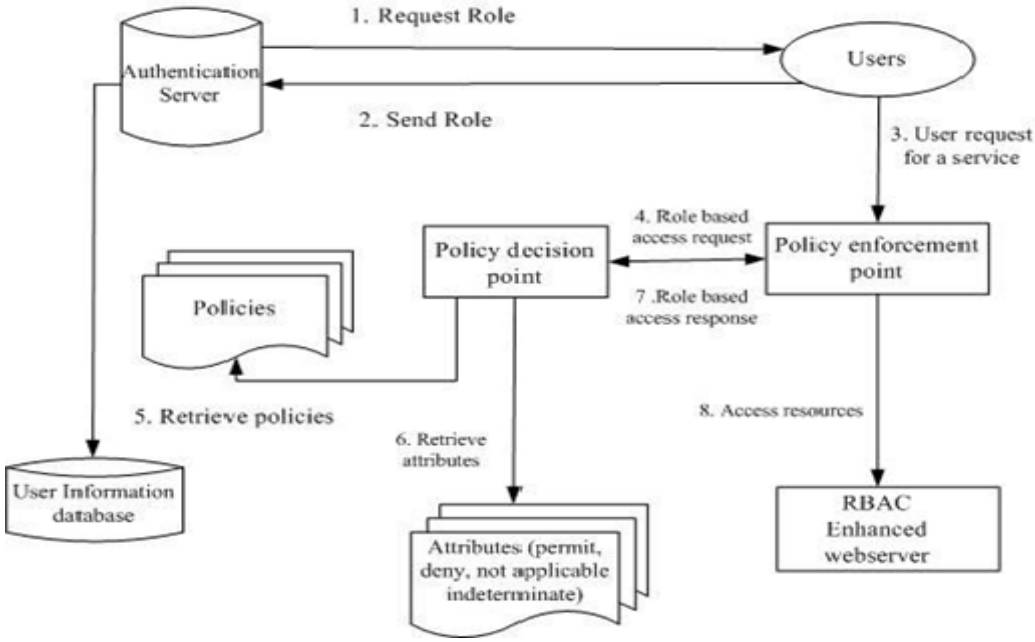

Figure 3: Role of Server

to authenticated users and administrators, which improves implementation. To validate trust value, a C# and. net-based framework was introduced. A SQL database-maintained history of trust value and activities is stored in the database according to the four factors mentioned above. Malicious activity from unauthorized users logged into the database. Due to the high-speed performance of the SQL database, calculations for data could be made in seconds. Administrators have the right to check the trust audit logs. A trust value of 0 to 0.5 is considered low, and 0.5 to 1 is high. At the time of login, the current framework calculates the trust value of every user. The value of EHS increases as the system becomes more mature.

Let's say for EHS of 100 employees, the number of incidents with ACM is say 20, and the number of incidents with $rTrust$ is not present, then the security will be in Eq 1

$$1 - \frac{ACModuleCase + 1}{ACModuleCase + 2} \tag{1}$$

$1-[20+1/(20+2)] = 1-(21/22) = 4.54$ hence security is very low. Let's say for an EHS of 100 employees, the number of incidents with the AC module is say 20, and the number of incidents with $rTrust$ is 130. Then security improvement will be in Eq 2.

$$1-(rTrustCases)+\frac{1}{ACModuleCase + 2}+ACModuleCases+2 \tag{2}$$

$1-[130+1/(130+20+2)] = 1-(131/152) = 13.81$ hence 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 AC module is say 20, and the number of incidents with $rTrust$ is 30 then Improvement in security will be in Eq 3.

$$1-(rTrustCases)+\frac{1}{rTrustCases + ACModuleCase}+2 \tag{3}$$

$1-[30+1/(30+20+2)] = 1-[101/122] = 40.38\%$, hence security is improved as employees are aware of unauthorized activities. The current work goes under the dynamic AC module in which the administrator controls users and checks the trust value of all users. Here rTrust model is used for the calculation of user trust. To achieve high trust some parameters, need to guarantee that stored time is matched with accessed time like, leave time, on-duty time emergency time, etc. The system interacts multiple times with the user at every interval. Here's a two-way possibility either store time matched with access time or mismatched. (ATmis) showed mismatched and (ATmat) showed matched in Eq 4 and possible trust value of requested user calculated below.

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

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

The behavior of users directly connects with the user feedback in the system, and feedback is in two ways either positive or negative. Here assumes the feedback value is between 0 to 0.5 in low feedback and for high feedback the value is 0.5 to 1 and possible feedback trust (Tfeed) is in Eq 5.

$$Tfeed = \frac{FEEDhigh + 1}{FEEDhigh + FEEDlow + 2} \tag{5}$$

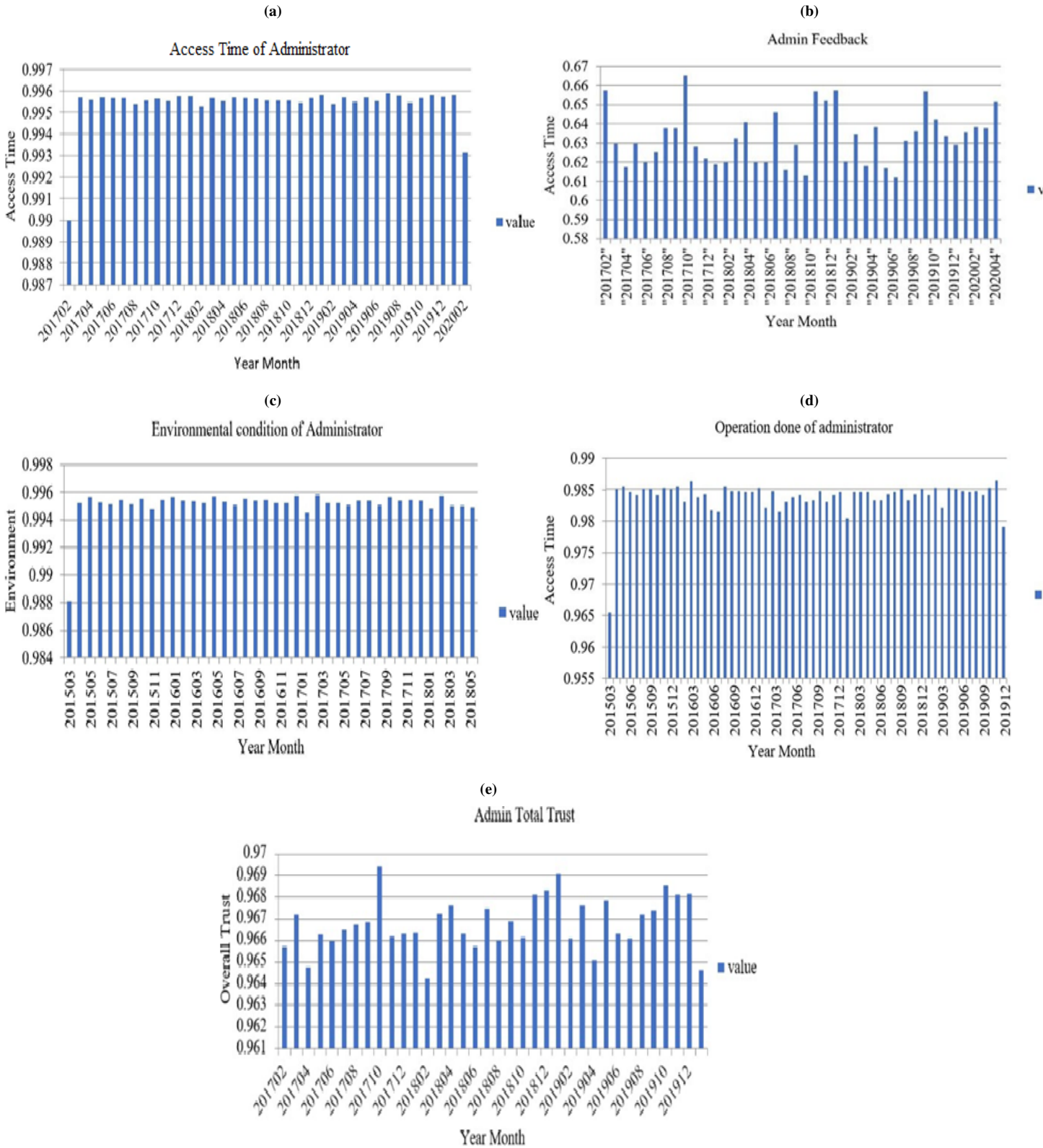

Figure 4: (a) Total Access Time of Administrator, b). Administrator Feedback, c) Environmental Condition Data Check by Administrator, d) Operations Done from Administrator, e) The Admin Total Trust

Where high feedback, denoted by FEEDhigh, and low feedback, denoted by FEEDlow, represent the total amount of high and low feedback, respectively. The admin feedback is graphically illustrated in Figure 4b. In the system, sometimes the user might perform a few unauthorized operations, trust is also calculated based on authorized operations or unauthorized operations executed by the requested user. Possible trust on the base of operation performed (Top) is shown in Eq 6.

$$Top = \frac{OP_auth + 1}{OP_auth + OP_unauth + 2} \tag{6}$$

Where OP_auth and OP_unauth represent, respectively, the total number of authorized operations and unauthorized operations. OP_auth is the authorized operations count. The environmental condition also depends on the trust degree and is checked during access time, if the user login or accesses the healthcare data from its registered location then the trust degree of the user is high as shown in Figure 4c. Possible trust on the basis of environmental condition (Tec) is in Eq 7 and checked in two ways i.e., True or False.

$$Tec = \frac{EC_true + 1}{EC_true + EC_false + 2} \tag{7}$$

Where EC_true represents the total number of times the user accesses the data while they are within the registered location, and EC_false represents the amount of time the user accessed the data while they were in a location that was not registered. The following formula as shown in Eq 8 is used to determine the overall user trust value (Tu-overall) of a requested user 'u' for the purpose of accessing the data:

$$Tu - overall = \frac{\alpha 1.UTEP1 + \alpha 2.UTEP2 + \alpha 3.UTEP3}{+\alpha 1.Tat + \alpha 2.Tfeed + \alpha 3.Top + \alpha.Tec} \tag{8}$$

Where $\alpha 1$ + $\alpha 2$ + $\alpha 3$ +....+ $= 1$, and $\alpha 1$ + $\alpha 2$ + $\alpha 3$ + ...+αk are the weights for each UTEP with Tec Model. Because the trust value of the user is taken into consideration by the AC module before deciding whether or not to grant access to the user, the level of security is improved.

It is, however, acceptable to compromise a certain accuracy rate when compared to the losses generated by system crashes. This is done to ensure that the system and resources are constantly in a somewhat safe state and to prevent higher losses. Due to the fact that the risk assessment prevents the system resources from being overused during the recovery phase, this system is able to recover from the anomaly more quickly than any other system. The preceding experiments have shown that the optimized role-based access control using trust mechanisms in an e-health cloud environment that was proposed in this paper is able to perform a risk assessment on requests according to the dynamic changes of subjects, resources, and environments and make corresponding decisions. As a result, it is able to dynamically protect the system and resources in a relatively secure state, which helps prevent system crashes and greater losses. The method of evaluation is straightforward, useful, and has a high degree of practicability. The access control approach that has been proposed is excellent for ensuring the safety of cloud-based dynamic medical data storage, processing, and accessibility.

A. PARAMETER MEASUREMENTS FROM ADMINISTRATOR

Here graphs are presented of administrator access time inFigure 4a, feedback of administrator in Figure 4b, environment condition check by administrator in Figure 4c, and operation done from administrator in Figure 4d.

In Figure 4e graph represents the total admin trust and complete confidence of executives. Here values of confidence are calculated from 0 to 1. To calculate admin total trust following Eq 9 and method was used.

$$Total_{trust} = \alpha 1 Taut + \alpha 2 + Tfeed + \alpha 3 Tec + \alpha 4 Top \tag{9}$$

here, $\alpha 1 = 0.3189, \alpha 2 = 0.064, \alpha 3 = 0.4512, \alpha 4 = 0.1657 and \alpha 1 + \alpha 2 + \alpha 3 + \alpha 4 = 1$

B. MATHEMATICAL PROOF FOR OPTIMIZATION OF ACCESS CONTROL

The mathematical proof describes the approach taken to optimize access control in the RBAC system with the trust mechanism that is proposed. The primary objective is to reduce the average response time for user requests. Trust levels, resource allocation, role activation, and permission assignment are all taken into account in order to implement an effective and secure access control system within the E-Health Cloud Environment. Our objective is to reduce the average response time (AR) for user inquiries, which can be expressed as represented in Eq 10 :

$$AR = \frac{1}{|X|} \sum_{x \in X} A(x) \tag{10}$$

subject to:

1) **Restrictions on the Assignment of Role Permissions:** It is imperative to verify that every role r possesses the requisite permissions in order to execute its designated duties.

$$\forall r \in R, \forall p \in P : \text{Role Permission}(r, p) \in \{0, 1\}$$

2) **Limitations on Trust Mechanisms:** Develop a hierarchy of trust between roles and users.

$$\forall u \in X, \forall r \in R : \text{Trust Level}(u, r) \in [0, 1]$$

3) **Limitations on Role Activation:** Per user, specify which roles are active in accordance with their trust level.

$$\forall u \in X, \forall r \in R : \text{Active Role}(u, r) \in \{0, 1\}$$

4) **Implications for Resource Allocation:** Before proceeding, ensure that system resources are allocated effectively.

$$\sum_{r \in R} \text{Resource Allocation}(r) \leq \text{Total Resources}$$

C. ALGORITHM: TRUST-BASED ACCESS CONTROL OPTIMIZATION

This section introduces the Trust-Based Access Control Optimization (TBACO) algorithm, which plays a crucial role in optimizing access control in the proposed RBAC system that incorporates a trust mechanism. The TBACO algorithm prioritizes the reduction of the average response time (AR) for user queries, while simultaneously guaranteeing effective access control inside the E-Health Cloud Environment.

Input:

- Users, X
- Roles, R
- Permissions, P
- Trust Levels, $TrustLevel(u, r)$ for each u in X and r in R
- Resource Allocation, $ResourceAllocation(r)$ for each r in R
- Total Resources

Output: Optimized Role-Permission Assignments

Procedure: TBACO

```
Initialize Role-Permission
for each $r$ in $R$, each $p$ in $P$:
    $RolePermission(r, p) = 0$ or $1$

Calculate Trust-Scores
for each $u$ in $X$, each $r$ in $R$:
    Calculate $TrustLevel(u, r)$ based on
    historical user behavior and feedback

Role-Activation
for each $u$ in $X$:
    for each $r$ in $R$:
        Determine $ActiveRole(u, r)$ based on
        $TrustLevel(u, r)$
        if $TrustLevel(u, r) \geq Threshold$:
            $ActiveRole(u, r) = 1$
        else:
            $ActiveRole(u, r) = 0$

Resource-Allocation
for each $r$ in $R$:
    $ResourceAllocation(r) = CalculateResource
    Allocation(r, ActiveRole)$

Access Control Optimization
while resources are available:
    for each $u$ in $X$:
        Select an active role $r$ that
        minimizes access latency for the
        user's request Calculate access
        latency $A(x)$ based on
        $RolePermission$ and $Resource
        Allocation$
        Update $RolePermission$ for $r$
        based on the request

Termination
Repeat the access control optimization
process until a
predetermined number of iterations
Return the optimized
Role-Permission Assignments
```

D. PRIVACY AND SECURITY MEASURES

It is a well-known truth that the move from conventional healthcare systems to e-healthcare has brought with it a lot of benefits and has made healthcare systems easier and more economical. On the other hand, there are a lot of issues involved with it, such as maintaining the confidentiality, privacy, and security of patients' records. Cloud computing is widely recognized as an acceptable form of digital technology that is currently seeing widespread application in the field of healthcare. Cloud service providers and other government organizations have collaborated to develop a comprehensive set of security rules and procedures in the hopes of boosting the level of trust that patients and organizations have in cloud computing. The servers that are housed in the cloud have been widely divided into three categories: trusted, semi-trusted, and untrusted. It is possible to describe a trustworthy server as one in whom one can place one's whole faith. It does not result in any information being leaked and poses no risk to the data that pertains to health. The servers that fall into the category of semi-trusted are those that have a reputation for being truthful but nosy. They connive with malevolent users in order to obtain personal health information. Untrusted servers are unreliable and have a high risk of being compromised by an adversary. The following are some of the ways in which the e-health system has a requirement for security and privacy:

- Data integrity is a mechanism that ensures personal health information is not changed by an unauthorized entity. This process is also known as "data integrity."
- Data confidentiality: This is a technique that ensures sensitive health information does not reach unauthorized people. It does this by keeping the information from leaking out. Encryption of data is a method for protecting its confidentiality.
- Authenticity: It is a technique that ensures sensitive health data is accessed only by authorized and authentic authorities. This safeguard ensures that patients' privacy is protected.
- Accountability is a system for justifying the acts and decisions of organizations and individuals. It may be thought of as a way to hold people to account.

- Audit: It maintains a record of all activity that takes place on the health data and ensures that it is continuously monitored and safeguarded. Additionally, it protects the confidentiality and safety of the data.
- Non-repudiation refers to the fact that both the sender and the receiver do not deny the legitimacy of the message. This indicates that neither patients nor doctors will be able to refute health data after it has been stolen.
- Anonymity: This feature is a method that conceals the identities of the users, making it impossible for the cloud servers to access the information that has been stored on the users' health.

V. DISCUSSION

A. ASSESSING THE TRUST-CENTRIC FRAMEWORK IN HEALTHCARE DATA MANAGEMENT

Healthcare data security has persistently been a topic of paramount concern, urging robust frameworks prioritizing trust, access, and data protection. The presented trust-centric approach places healthcare users (HCU) at the center of the data access landscape, surrounded by a series of checks, authentications, and trust evaluations. Drawing parallels with existing literature, most traditional systems put emphasis predominantly on just access rights, relying heavily on mere credential verification. However, our framework brings in the unique Trust-Evaluation Centre (TEC), a game-changer that adds a layer of trust assessment. This innovation ensures not only whether the user has the right credentials but also if they have historically maintained the trustworthiness to access data. Such an introduction is vital in healthcare, where data sensitivity is unparalleled. Figures and results illustrate the meticulous steps involved in this framework. The pivotal role of the Authentication Server stands out, verifying user credentials from a stored database. While this is a standard procedure in most systems, the subsequent trust evaluation sets our framework apart. Incorporating a trust rating between 0 and 1 is intuitive, ensuring a gradient rather than a binary assessment of trustworthiness. The role of trust, as depicted in the figures, evidently outlines that trust isn't merely black and white; it's a spectrum. This nuanced approach mimics real-world scenarios where trustworthiness isn't a mere yes or no but varies based on past interactions. The equations presented underline the mathematical rigor underpinning the trust calculations. The system ensures a comprehensive trust assessment by accounting for factors like matched access time, feedback, operations performed, and even the environmental conditions during data access. This multifaceted approach ensures trust isn't just about past interactions and real-time contextual information. Yet another commendable feature is the dynamic nature of the Access Control (AC) module. Administrators can actively monitor and adjust trust values, balancing data protection and necessary data access. The various graphs representing administrator metrics testify to the depth of control and monitoring possible with this framework. While our model showcases significant advancements, it also builds upon the lessons learned from previous models. For instance, the RBAC models, prevalent in many current systems, serve as a foundation. Still, our model takes it a step further by incorporating dynamic trust evaluations.

B. ADVANCING BEYOND EXISTING SOLUTIONS

Comparing our framework with existing state-of-the-art studies, we've effectively merged the concepts of multifactor authentication and dynamic trust modeling. SQL Server provides a reliable backend database system, ensuring data sanctity while offering high-speed performance. Additionally, the fusion of the C# and . NET-based framework for trust validation stands as a modern solution, harmoniously integrating various technologies. In conclusion, while the trust-centric framework for healthcare data management showcased here has pioneered several advancements, there's always room for improvement, as highlighted by some of its limitations. However, the steps taken in this study towards creating a more secure, dynamic, and trust-based system are undeniable. Future research can potentially address these limitations, making this an even more formidable solution in the realm of healthcare data security.

C. LIMITATIONS AND FUTURE DIRECTIONS

The research's focus on a trust-centric approach to healthcare data access, while novel, does come with certain limitations. First and foremost, its applicability across larger healthcare entities is still unproven, leading to potential questions about scalability. The subjective nature of trust complicates its precise measurement, even when using our advanced mathematical models. There's also a risk in relying too heavily on the system's trust assessments, as a high trust rating doesn't necessarily equate to the absence of malevolent intentions. Introducing environmental variables during data access may inadvertently lead to biases, and the adaptable nature of the Access Control component might result in added operational costs. Additionally, if feedback systems aren't meticulously refined, they become prone to errors. The system's reliance on specific tech platforms like SQL Server, C, and .NET might hinder its broader adoption.

In the future, our focus will be refining the system for more extensive institutional networks, incorporating forward-thinking machine learning techniques, and bolstering user understanding of the system's functionalities. It may be beneficial to explore combined trust frameworks to develop a more resilient system and to refine feedback procedures to uphold their precision consistently. It's also essential for subsequent versions to aim for enhanced interoperability and retain a pronounced ethical perspective, assuring a harmonious blend of security and ethical data practices in the healthcare sector.

D. COMPARISON WITH STATE-OF-ART EXISTING STUDIES

The healthcare sector's increasing reliance on cloud technology has ushered in innovations and challenges. Traditional systems, while robust, often lack fine-grained permis-

TABLE 1: Comparison of Proposed Study with Existing Relevant Study

Performance Parameter	Proposed Study	Existing Relevant Study
Data Security	Enhanced through TEC and RBAC.	Emphasizes encryption and firewalls.
User Trust Assessment	Integrated Trust-Evaluation Centre (TEC).	No explicit user trust evaluation.
Authentication Speed	.Net-based rigorous authentication.	Standard authentication mechanisms.
User Role Assignment	Dynamic roles based on user behavior.	Static roles with predefined permissions.
Response Time	Optimized for prompt responses.	Not specified or optimized.
Granularity of Access Control	Fine-grained, role-based permissions.	Basic access control mechanisms.
User Experience Generalized approach with standard setup.	Tailored with the balance of access	security.
Cloud Environment	Centralized, Intertwined Healthcare Data mgmt.	Cloud-based implementation not discussed.
Trustworthiness Management	Trust mechanism based on behavioral analysis.	Trust not a major focus of the study.
Scalability	Not extensively discussed in the study.	Not discussed or not focused on.

sion management, resulting in potential vulnerabilities. The proposed study introduces an advanced trust mechanism, uniquely blending RBAC with behavioral analytics. Unlike its predecessors, this model dynamically observes user behavior to assign roles, ensuring more responsive access controls. This study showcases a marked advancement over traditional approaches by addressing the limitations in permission granularity, enhancing system responsiveness through behavioral insights, and deploying a .net-based framework for rigorous user authentication. It offers a proactive model in healthcare data management, prioritizing security and user experience. In essence, the proposed model promises a future of healthcare data systems that are safer, more efficient, and more attuned to user needs, setting it distinctly apart from existing methodologies. A detailed comparison of the proposed study with the existing state-of-the-art studies may be viewed in Table 1.

VI. CONCLUSION

Multiple issues exist in different EHSs. Protection of EHS data is a wide research area in the current era, and many solutions are proposed against various attacks. This study suggested a solution, namely RBAC, which is much more sufficient than other solutions in the market. This study provides a combination of AC module with trust mechanism and overcome security issues in existing AC module. The trust degree level is joined with the requested user in the RABC model and monitors the user behavior. Depending on user behavior roles are assigned to users. The AC module is implemented by using an SQL server, where the administrator controls the access to various modules of EHS. For the validation of trust value, a framework of .net based introduced. This EHS framework certified to its customers that their information is safe from unauthorized users and security threats. Some limitations of this work are also here like, if more than 100 users request EHS simultaneously, the response time is a little bit slow, and more trust parameters are needed here.

FUNDING

This research received no specific funding from any funding agency

CONFLICT OF INTEREST

The authors declare that they have no Conflict of interest.

ACKNOWLEDGMENTS

The authors are also thankful to AIDA Lab CCIS Prince Sultan University, Riyadh Saudi Arabia for support.

REFERENCES

[1] N. A. Azeez and C. Van der Vyver. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2):97–108, 2019.

[2] Tariq Mahmood, Jianqiang Li, Yan Pei, Faheem Akhtar, Azhar Imran, and Khalil Ur Rehman. A brief survey on breast cancer diagnostic with deep learning schemes using multi-image modalities. IEEE Access, 8:165779–165809, 2020.

[3] Muhammad Attique Khan, Muhammad Imran Sharif, Mudassar Raza, Almas Anjum, Tanzila Saba, and Shafqat Ali Shad. Skin lesion segmentation and classification: A unified framework of deep neural network features fusion and selection. Expert Systems, 39(7):e12497, 2022.

[4] Louis Leung and Cheng Chen. E-health/m-health adoption and lifestyle improvements: Exploring the roles of technology readiness, the expectation-confirmation model, and health-related information

activities. Telecommunications Policy, 43(6):563–575, 2019.

[5] Nazar Hussain, Muhammad Attique Khan, Muhammad Sharif, Sajid Ali Khan, Abdulaziz A Albesher, Tanzila Saba, and Ammar Armaghan. A deep neural network and classical features based scheme for objects recognition: an application for machine inspection. Multimedia Tools and Applications, pages 1–23, 2020.

[6] Tariq Mahmood, Amjad Rehman, Tanzila Saba, Lubna Nadeem, and Saeed Ali Omer Bahaj. Recent advancements and future prospects in active deep learning for medical image segmentation and classification. IEEE Access, 2023.

[7] Ghulam Muhammad, Saad Naveed, Lubna Nadeem, Tariq Mahmood, Amjad R Khan, Yasar Amin, and Saeed Ali Omer Bahaj. Enhancing prognosis accuracy for ischemic cardiovascular disease using k nearest neighbor algorithm: A robust approach. IEEE Access, 2023.

[8] Shekha Chenthara, Khandakar Ahmed, Hua Wang, and Frank Whittaker. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 7:74361–74382, 2019.

[9] Saeed Iqbal, Adnan N Qureshi, Jianqiang Li, Imran Arshad Choudhry, and Tariq Mahmood. Dynamic learning for imbalance data in learning chest x-ray and ct images. Heliyon, 2023.

[10] Weiran Liu, Xiao Liu, Jianwei Liu, Qianhong Wu, Jun Zhang, and Yan Li. Auditing and revocation enabled role-based access control over outsourced private ehrs. In 2015 IEEE 17th international conference on high performance computing and communications, 2015 IEEE 7th international symposium on cyberspace safety and security, and 2015 IEEE 12th international conference on embedded software and systems, pages 336–341. IEEE, 2015.

[11] Ayesha Jabbar, Shahid Naseem, Tariq Mahmood, Tanzila Saba, Faten S Alamri, and Amjad Rehman. Brain tumor detection and multi-grade segmentation through hybrid caps-vggnet model. IEEE Access, 2023.

[12] Muhammad Imran Khan, Azhar Imran, Abdul Haleem Butt, Ateeq Ur Rehman Butt, et al. Activity detection of elderly people using smartphone accelerometer and machine learning methods. 2021.

[13] Tanzila Saba. Automated lung nodule detection and classification based on multiple classifiers voting. Microscopy research and technique, 82(9):1601–1609, 2019.

[14] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon. A survey on internet of things and cloud computing for healthcare. Electron., 8(7):1–49, 2019.

[15] C. A. Ardagna, S. De Capitani Di Vimercati, S. Foresti, T. W. Grandison, S. Jajodia, and P. Samarati. Access control for smarter healthcare using policy spaces. Computers & Security, 29(8):848–858, 2010.

[16] Saeed Iqbal, Adnan N. Qureshi, Jianqiang Li, and Tariq Mahmood. On the analyses of medical images using traditional machine learning techniques and convolutional neural networks. Archives of Computational Methods in Engineering, 30(5):3173–3233, 2023.

[17] M. Ashtiani and M. Abdollahi Azgomi. Trust modeling based on a combination of fuzzy analytic hierarchy process and fuzzy vikor. Soft Computing, 20(1):399–421, 2016.

[18] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang. A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6):4682–4696, 2020.

[19] Randhir Kumar and Rakesh Tripathi. Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. the Journal of Supercomputing, pages 1–40, 2021.

[20] Ahmad Taher Azar. Hybrid machine learning approach for human activity recognition. International Journal of Computer Applications in Technology, 72(3):231–239, 2023.

[21] Rabie A Ramadan, Ahmed Y Khedr, Kusum Yadav, Eissa Jaber Alreshidi, Md Haidar Sharif, Ahmad Taher Azar, and Hiqmet Kamberaj. Convolution neural network based automatic localization of landmarks on lateral x-ray images. Multimedia Tools and Applications, 81(26):37403–37415, 2022.

[22] P Chinnasamy and P Deepalakshmi. Hcac-ehr: hybrid cryptographic access control for secure ehr retrieval in healthcare cloud. Journal of Ambient Intelligence and Humanized Computing, pages 1–19, 2022.

[23] P Chinnasamy, P Deepalakshmi, and K Shankar. An analysis of security access control on healthcare records in the cloud. In Intelligent Data Security Solutions for e-Health Applications, pages 113–130. Elsevier, 2020.

[24] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand. Security techniques for the electronic health records. Journal of Medical Systems, 41(8), 2017.

[25] Mustafa Abdul Salam, Ahmad Taher Azar, and Rana Hussien. Swarm-based extreme learning machine models for global optimization. Computers, Materials & Continua, 70(3), 2022.

[26] A. Singh and K. Chatterjee. Itrust: identity and trust based access control model for healthcare system security. Multimedia Tools and Applications, 78(19):28309–28330, 2019.

[27] Hany Atlam, Ahmed Alenezi, Robert Walters, Gary Wills, et al. An overview of risk estimation techniques in risk-based access control for the internet of things. 2017.

[28] Nawaf Alharbe, Abeer Aljohani, Mohamed Ali Rakrouki, and Mashael Khayyat. An access control model based on system security risk for dynamic sensitive data storage in the cloud. Applied Sciences, 13(5):3187, 2023.

[29] Tariq Mahmood, Jianqiang Li, Yan Pei, and Faheem Akhtar. An automated in-depth feature learning algorithm for breast abnormality prognosis and robust characterization from mammography images using deep transfer learning. Biology, 10(9):859, 2021.

[30] Kamesh and N. Sakthi Priya. A survey of cyber crimes. Security and Communication Networks, 5(June):422–437, 2012.

[31] L. P. Suresh, S. S. Dash, and B. K. Panigrahi. Artificial intelligence and evolutionary algorithms in engineering systems: Proceedings of ICAEES 2014, Volume 2, volume 325. 2015.

[32] R. K. Banyal, V. K. Jain, and P. Jain. Dynamic trust based access control framework for securing multi-cloud environment. ACM International Conference Proceeding Series, 11-16-Nove, 2014.

[33] T. Bhattasali, R. Chaki, N. Chaki, and K. Saeed. An adaptation of context and trust aware workflow oriented access control for remote healthcare. International Journal of Software Engineering and Knowledge Engineering, 28(6):781–810, 2018.

[34] Daniel Ricardo Dos Santos, Carla Merkle Westphall, and Carlos Becker Westphall. A dynamic risk-based access control architecture for cloud computing. In 2014 IEEE network operations and management symposium (NOMS), pages 1–9. IEEE, 2014.

[35] Juan Li, Yan Bai, and Nazia Zaman. A fuzzy modeling approach for risk-based access control in ehealth cloud. In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pages 17–23. IEEE, 2013.

[36] Hany F Atlam, Muhammad Ajmal Azad, and Nawfal F Fadhel. Efficient nfs model for risk estimation in a risk-based access control model. Sensors, 22(5):2005, 2022.

[37] Hany F Atlam, Muhammad Ajmal Azad, Madini O Alassafi, Abdulrahman A Alshdadi, and Ahmed Alenezi. Risk-based access control model: A systematic literature review. Future Internet, 12(6):103, 2020.

[38] Abhishek Kesarwani and Pabitra Mohan Khilar. Development of trust based access control models using fuzzy logic in cloud computing. Journal of King Saud University-Computer and Information Sciences, 34(5):1958–1967, 2022.

[39] Guoyuan Lin, Danru Wang, Yuyu Bie, and Min Lei. Mtbac: A mutual trust based access control model in cloud computing. China Communications, 11(4):154–162, 2014.

[40] Li Chunge, Ma Mingji, Li Bingxu, and Chen Shuxin. Design and implementation of trust-based access control model for cloud computing. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), volume 5, pages 1934–1938. IEEE, 2021.

[41] Yuchen Wu and Pingping Liu. Research on trust-role access control model in cloud computing. International Journal of Advanced Network, Monitoring and Controls, 4(2):75–80, 2019.

[42] Ichiro Satoh. Context-aware access control model for services provided from cloud computing. Intelligent Distributed Computing XI, pages 285–295, 2018.

[43] D. Gupta, S. Bhatt, M. Gupta, O. Kayode, and A. S. Tosun. Access control model for google cloud iot. In Proceedings - 2020 IEEE 6th International Conference on Big Data Security, Cloud, and 2020 IEEE International Conference on High Performance and Smart Computing, BigDataSecurity/HPSC/IDS, pages 198–208, 2020.

[44] F. M. Okikiola, A. M. Mustapha, A. F. Akinsola, and M. A. Sokunbi. A new framework for detecting insider attacks in cloud-based e-health care system. 2020 International Conference on Mathematics, Computer Engineering and Computer Science (ICMCECS), 2020.

[45] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty. Interoperability and synchronization management of blockchain-based decentralized e-health systems. IEEE Transactions on Engineering Management, 67(4):1363–1376, 2020.

[46] A. P. G. Lopes and P. R. L. Gondim. Mutual authentication protocol for d2d communications in a cloud-based e-health system. Sensors (Switzerland), 20(7), 2020.

[47] V. Rivera. Formal verification of access control model for my health record system. In Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems (ICECCS), volume 2020-October, pages 21–30, 2020.

[48] D. L. Chiang, Y. T. Huang, T. S. Chen, and F. P. Lai. Applying time-constraint access control of personal health record in cloud computing. Enterprise Information Systems, 14(2):266–281, 2020.

[49] L. O. Nweke, P. Yeng, S. D. Wolthusen, and B. Yang. Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. International Journal of Advanced Computer Science and Applications, 11(2):683–690, 2020.

[50] A. Singh, U. Chandra, S. Kumar, and K. Chatterjee. A secure access control model for e-health cloud. In 2019 IEEE Region 10 Annual International Conference (TENCON), pages 2329–2334, 2019.

[51] R. Sivan and Z. A. Zukarnain. Security and privacy in cloud-based e-health system. Symmetry, 13(5), 2021.

[52] T. Kanwal, A. Anjum, and A. Khan. Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Cluster Computing, 24(1):293–317, 2021.

[53] C. Anilkumar and S. Subramanian. A novel predicate based access control scheme for cloud environment using open stack swift storage. Peer-to-Peer Networking and Applications, 2020.

ATEEQ UR REHMAN BUTT is working as an Instructor (Computer Science) in the Punjab School Education Department. He also served as CTI (Computer Science) in the Punjab Higher Education Department. He did his BS (Hons) in Information Technology from the University of Education Township, Lahore, & MS (Computer Science) from the National Textile University, Faisalabad. He has authored 1 book on Computer Science & 9 research papers in reputed IF journals and conferences (ACM & IEEE). His research interests include Artificial Intelligence, Machine Learning, Deep Learning, Image Processing & Health Informatics.

DR. TARIQ MAHMOOD is an Assistant Professor/HOD at the Faculty of Information Sciences, University of Education, Vehari Campus, Vehari, Pakistan. He has completed his doctoral degree in Software Engineering from the Beijing University of Technology, China, and his master's degree in computer science from the University of Lahore, Pakistan. He is a renowned expert in Image Processing, Healthcare Informatics and Social Media Analysis, Adhoc Networks, WSN. He has contributed 40+ research articles in well-reputed international journals and conferences. He is the editorial member and reviewer of various journals, including Plos One, Journal of Supercomputer, Journal of digital Imaging, International Journal of Sensors, Wireless Communications and Control, etc. His research interests include Image Processing, Social Media Analysis, Medical Image Diagnosis, Machine Learning, and Data Mining. He aims to contribute to interdisciplinary research of computer science and human-related disciplines. Email: tmsherazi@ue.edu.pk Affiliation: Faculty of Information Sciences, University of Education, Vehari Campus, 61100, Vehari

PROF. DR. TANZILA SABA (Senior Member, IEEE) received a Ph.D. degree in document information security and management from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, in 2012. She is an Associate Chair with the Information Systems Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia, where she is the Artificial Intelligence and Data Analytics Research Laboratory Leader. Her primary research interests include medical imaging, pattern recognition, data mining, MRI analysis, and soft computing. She is an Active Professional Member of ACM, AIS, and IAENG organizations. She is the PSU Women in Data Science (WiDS) Ambassador at Stanford University and the Global Women Tech Conference. She was a recipient of the Best Student Award from the Faculty of Computing, UTM, in 2012

DR. SAEED ALI OMER BAHAJ is Associate Professor Department of Management Information Systems College of Business Administration In Alkharj. Dr. Saeed Ali Bahaj is Associate Professor in Computer Engineering Department at Hadramout University Yemen and MIS Department COBA Prince Sattam bin Abdul-Aziz. He earned a doctoral at Pune University, India, in 2006. His main research interests include Artificial Intelligence, information management, forecasting, information engineering, big data, and information security.

DR. AMJAD R KHAN (Senior Member, IEEE) received the Ph.D. and Postdoctoral degrees (Hons.) from the Faculty of Computing, Universiti Teknologi Malaysia, with a specialization in forensic documents analysis and security, in 2010 and 2011, respectively. He is a Senior Researcher with the Artificial Intelligence and Data Analytics Laboratory, College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh, Saudi Arabia. He is the author of more than 200 ISI journal articles and conferences. Currently, he is a PI in several funded projects and also completed projects funded from MOHE Malaysia and Saudi Arabia. His research interests include data mining, health informatics, and pattern recognition. He received the Rector Award for the 2010 Best Student from Universiti Teknologi Malaysia.

PROF. DR. MUHAMMAD WASEEM IQBAL has completed his PhD in Computer Science from "The Superior University" Lahore, Pakistan. Currently he is working as an Professor in the Software Engineering Department. He is an active researcher and has more than 50 research publications in well reputed Journals and conferences. Further, he has more than sixteen years of teaching and research experience in well reputed institutions. He specializes in Human Computer Interaction (HCI), with special interest in Adaptive Interfaces (AI), User's Context, UX/UI for normal and visual impaired people and User Centered Design (UCD). He has also interested in Internet of Things (IoT), Internet of Medical Things (IoMT), Human Centric Artificial Intelligence (HCAI), Semantic relations and Ontological modeling.

FATEN S. ALAMRI received the Ph.D. degree in system modeling and analysis in statistics from Virginia Commonwealth University, USA, in 2020. Her Ph.D. research included Bayesian dose-response modeling, experimental design, and non-parametric modeling. She is an Assistant Professor at the Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdul Rahman University. Her research interests include spatial area, environmental statistics, and brain imaging.