IJBPAS, November, Special Issue, 2021, 10(11): 773-782
ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)
'A Bridge Between Laboratory and Reader'

www.ijbpas.com

A NOVEL CLOUD-ASSISTED SECURE AND QUICK ACCESS CONTROL DATA PROTECTION MODEL IN HEALTHCARE

HARSHA SHASTRI. V[1*], SURAPANENI KRISHNA MOHAN[2], KAPOOR.R[3], JAMBERI.K[4], SYED KHASIM[5] AND J GNANA JESLIN[6]

1: Assistant Professor in Computer Science at Loyola Academy Opp. Suchitra X Roads, Secunderabad, Telangana, India

2: Departments of Biochemistry, Molecular Virology, Research, Clinical Skills & Simulation, Panimalar Medical College Hospital & Research Institute, Varadharajapuram, Poonamallee, Chennai - 600 123

3: Assistant Professor in Punjabi University Neighbourhood Campus, Jaito, Faridkot, India

4: Assistant Professor in Computer Science at S.A. College of Arts and Science, Veeraraghavapuram, India

5: Professor in Computer Science and Engineering at Dr.Samuel George Institute of Engineering & Technology, Markapur, Prakasam Dt, Andhra Pradesh, India

6: Assistant Professor, Department of CSE, RMK College of Engineering and Technology, Thiruvallur-601206, Chennai, Tamil Nadu

***Corresponding Author: Harsha Shastri.V; E Mail: harshashastri28@gmail.com**

Received 20th July 2021; Revised 22nd Aug. 2021; Accepted 30th Sept. 2021; Available online 1st Nov. 2021

https://doi.org/10.31032/IJBPAS/2021/10.11.1066

ABSTRACT

Deploying state-of-the-art technologies is vital and inevitable in the healthcare industry to cope with emerging services such as healthcare resource sharing and integration, collaborative consultation, and electronic health records. Cloud computing allows simple and easy user access, coping with users' dynamic and elastic demands, providing metered usage for its resources, and hence is increasingly being adopted by individual users as well as enterprise users. The Cloud is

being considered as an appropriate technology for future healthcare infrastructure. However, to use Cloud services effectively, users' data and/or resources have to be transferred to the cloud side and this inevitably raises several serious issues concerning losing control of users' resources, data privacy protection, data ownership, and security. This paper addresses security and privacy challenges in the healthcare cloud by deploying a novel framework with the Cloud Assisted Secure and Quick Access Control (CASQAC) model for controllability, traceability of data, and authorized access to system resources. Furthermore, the work seeks to develop a unique active auditing service that is capable of tracing, tracking, and triggering an alarm on any operation, data, or policy violations in the Cloud environment.

Keywords: Cloud computing, Cloud Assisted Secure and Quick Access Control, Monitor, Security, Healthcare

INTRODUCTION

Cloud computing has stepped into people's vision for many years, which has been widely considered as a large-scale distributed computing paradigm driven by economies of scale. It integrates and extends from existing Grid Technology, Service-Oriented Architecture, and Utility Computing Techniques **[1]**. By fusing a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, Cloud offers and delivers services on demand to external customers over the Internet **[2]**. Cloud computing is essentially characterized by functional segregation between available resources and users' PC: the computing resources normally reside outside the local environment, and the development and maintenance tasks related to provisioning the service are performed by the service provider **[3]**. People can leverage the cloud to store their documents online, share their information with friends, and consume more convenient and productive services with simple usage, fast access, and low cost on a remote server rather than physically local resources **[4]**. However, so far, the biggest obstacle of widespread adoption of cloud computing technology is data protection issues regarding security and privacy aspects due to its outsourced nature **[5]**.

To make effective use of Cloud services, users' data and/or resources have to be allocated to the cloud side. This pattern naturally raises several serious issues concerning losing controllability after users' resources are mandated in cloud center, and lacking appropriate scheme to address the

security and privacy issues such as preventing user's sensitive data from illegal disclosure or malicious violation, protection of data ownership, and personal information **[6-8]**. These issues surrounding cloud computing still have not been addressed satisfactorily, and for those reasons, cloud computing has not been widely adopted for serious applications, especially in the healthcare area. The recent researches on data protection regarding security and privacy issues in cloud computing have partially addressed some issues **[9]**. Data dispersal storage and secure retrieval scheme are some of the well-discussed approaches, which adopt some effective and flexible distributed algorithms to allocate users' data to diverse domains to guarantee correctness and integrity **[10]**. Although this scheme can efficiently decrease the risk of malicious data modification attacks and server colluding attacks, it reveals some drawbacks such as relying on complex algorithms and distributed management schemes that may bring in unnecessary computation and communication overhead, especially when data quantity is huge or existing frequent data operations **[11-12]**.

Related works

Another similar solution is a key distribution scheme based on public key infrastructure which applies cryptographic primitives and discloses decryption keys only to users who have authorized keys **[13]**. This general method satisfies the secure dynamic resource sharing scheme in cloud scenarios by distributing the decryption keys to the expected users. But one of the critical issues is the introduction of complexity in both key distribution and data encryption. The above two solutions can guarantee coarse-grained data protection in the cloud. However, to achieve a fine-grained data protection scheme, the new scheme is required to support some sophisticated context scenarios such as access condition time constraint or data operation purpose, etc. **[14]**. Data binding technology is another representative approach that encapsulates sensitive data with predefined policies to guarantee data protection centrally **[15]**. However, it is difficult to protect sensitive data against malicious modification or intrusive attacks with this structure due to its centralized nature.

To address the above schemes' weaknesses, we propose a novel data protection model which can be applied in distributed health cloud scenarios with low computational overhead but a solid data protection scheme **[16]**. This framework is based on CASQAC model and Active

Auditing Scheme (AAS). CASQAC extends the traditional Role-Based Access Control (RBAC) model and increases some new components which can achieve more sophisticated data protection scenarios including authorization delegation, resource sharing across different cloud servers, and context-based access control restricts consuming cloud service-based on the authorized token. Moreover, in contrast to some public auditing schemes in we rely on an AAS which can provide active ongoing monitoring and can automatically take actions based on a run-time scheme rather than on a probabilistic sampling technique periodically fetching the status of data.

Proposed system

A user, who subscribes to healthcare cloud services, is required to send his/her data along with associated access control policies to cloud services. The services will then grant access permissions to the data. Normally, the actions on data must be authorized according to the authentication of users through first security threshold which is the CASQAC service. Only valid users with authorized permission can access or modify the data, while unauthorized actions will be rejected by cloud services. It can guarantee the enforcement of CASQAC service without any violation. Besides that, once any operation, data, or policy violations are detected, an alert scheme can be triggered on a run-time basis.

Traditional access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) are difficult to ensure cloud data privacy protection. The RBAC model lacks context information to satisfy sophisticated scenarios. To achieve a robust data protection scheme that supports fine-grained data protection requirements in distributed healthcare cloud across multiple domains but does not rely on heavy communication and computation overhead, we propose the CASQAC model. Compared with other access control systems model introduces f new components: Organizations (Or), Conditions (Co), Obligations (Ob), Purposes (Pu) to enrich policy description for complicated usage requirements concerning authorization delegation, cross-realm role assignment, privacy-aware and active auditing scheme. The model is illustrated in **Figure 1**.

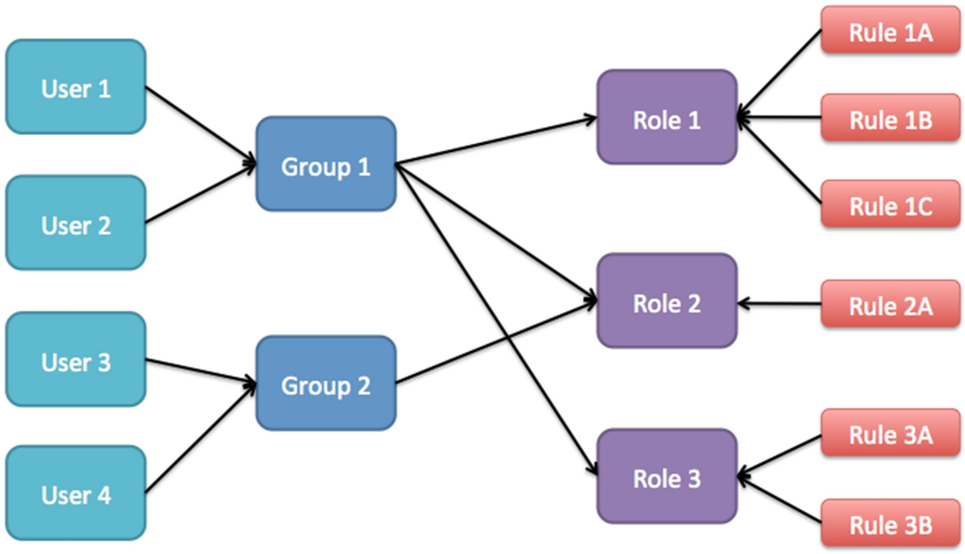

Figure 1: Model of CPRBAC

Role Assignment refers to an automatic procedure of authenticating healthcare user information and allocating the corresponding role to guarantee all associated operations on data are valid. approach in terms of role assignment is based on the notion of Attribute-Based Role Assignment (ABRA) which expresses the fact that the role of the user is associated with a 2-tuple including Subject and AttributeSet. Compared with the conventional subject-role assignment, ABRA is capable to satisfy dynamic role assignments based on some context information such as organization, domain, or time, etc., rather than simply achieving the corresponding relation between subject and role.

Role Hierarchy is an important notion in the RBAC model and it can efficiently reduce the total number of permission assignment costs. Normally, it defines an inheritance relationship among roles, which is similar to object-oriented programming terms. From the perspective of mathematic, role hierarchy is partial order that is a reflexive, transitive, and asymmetric relation. Role Delegation denotes permitting users to delegate certain capabilities to others under some restricted conditions. For instance, one specialist can delegate permission to an idle general practitioner when he is busy or unavailable. Note that the role delegation scheme only happens in a single domain. Role roaming refers to a role delegation scheme in a multiple-domain healthcare cloud environment. The scheme allows a user in an organization to gain external authentication information specified in

another organization through mirroring cross-domain roles.

Auditing Process

The above CASQAC service can guarantee healthcare cloud resources being accessed or managed legally according to formatted data protection policy, but such an access control scheme still requires an appropriate scheme to prevent deliberate data violation. Some security attacks still may deploy bugs or vulnerabilities of the system to illegally violate CASQAC service or directly bypass the access control layer to steal private information and maliciously modify users' data. Therefore, an active auditing scheme plays an important role in providing active ongoing monitoring and reporting functions against illegal operations on a runtime basis. To achieve this scheme, we establish an additional layer residing between the back-end data management layer and the CASQAC layer. This layer can be considered as a middleware module playing the role of proxy. **Figure 2** depicts the proxy and the active auditing scheme.

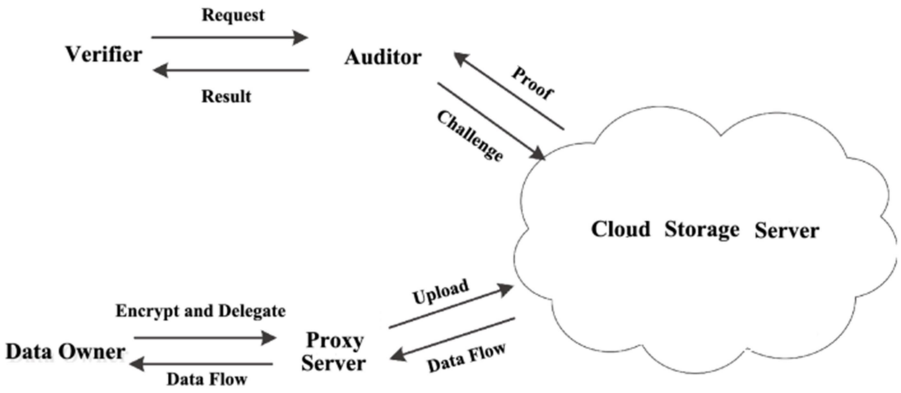

Figure 2: A scheme of Proxy and active auditing

This proxy offers two distinct interfaces, one is to receive request consisting of the response Ctx (response context information of CASQAC authorization result), the SQL request, and the proxy function that will be executed to trigger the report service to alert the violation event if the response is illegal against the SQL request. If the corresponding response Ctx is legal, the proxy will delegate the request to the back-end resource management system to fetch data. The response Ctx consists of a dynamic verification token, subject ID, data identifier, operation. The token is generated by a one-way hash function calculated by a 3-tuple dataset which contains the current timestamp (the validate period of the token is the 30s), 8-bit

random code (system keeps this random code for 30s in one authorization session), and subject ID. A valid token represents a current request is authorized by the CASQAC service, whereas an invalid or unknown token can be recognized simply through a reverse-verification process with the CASQAC service.

The other interface in proxy service is utilized to communicate with the database probe. We develop the probe component which is inside the Database (DB) server. Compared with polling service periodically capturing a snapshot of the existing status of DB, approach supports automatic action that can be triggered against policies violation without DB administrator intervention. This scheme relies on a secure bootstrapping to be run at the Operating System (OS) level, that is, any DB operations will be captured by the probe inside DB, but the probe is incapable to process the verification work, all information regarding query operations in DB will be transferred to proxy service for further verification with CASQAC service. Invalid behavior violating certain policies will be alerted by the report service to a specific data owner or administrator. Besides that, we create different functional trigger proxies according to the type of DB operations such as Select, Update, Delete, Insert, etc. to achieve filter and separate functions which achieve the smaller volume of information capturing, thereby reaching higher efficient auditing work. The following example is a select trigger

Implementation

We have implemented some parts of the data protection prototype including an authentication service and an authorization service based on CASQAC model. It deployed in Java and Java-encapsulated web service techniques, and all services can be invoked through published web interfaces. In the EHR viewer page, when a user requests an EHR read, the request will be analyzed by the CASQAC service to determine whether the user role and his/her access rights are valid. For example, if we define a policy.

Besides that, any operations on the DB can trigger probe in a real-time mode. The violation-detect service analyzes their execution with predefined policy. If illegal disclosure of data or malicious operations on data is encountered, the service will trigger a relevant report or procedure. **Figure 3** shows the monitoring screenshot on the administrator page. **Figure 4** shows the policy editing page. An administrator can authorize policy according to either policy template, or example format. The CASQAC service will analyze its legality.

Evaluation

Work concentrates on a solid data protection approach that becomes effective after data is transferred to the cloud. Computation security issues of cloud and network-level attack prevention are out of the range of research. An active auditing scheme can prevent policy violations and guarantee data disclosure. The data in cloud service is traceable with the active auditing scheme, and any illegal behavior over data can be alerted on a runtime basis. Data confidentiality and integrity do not discuss the cryptographic security methods. However, to enhance the confidentiality and integrity of data, a cryptographic-basis scheme is still necessary.

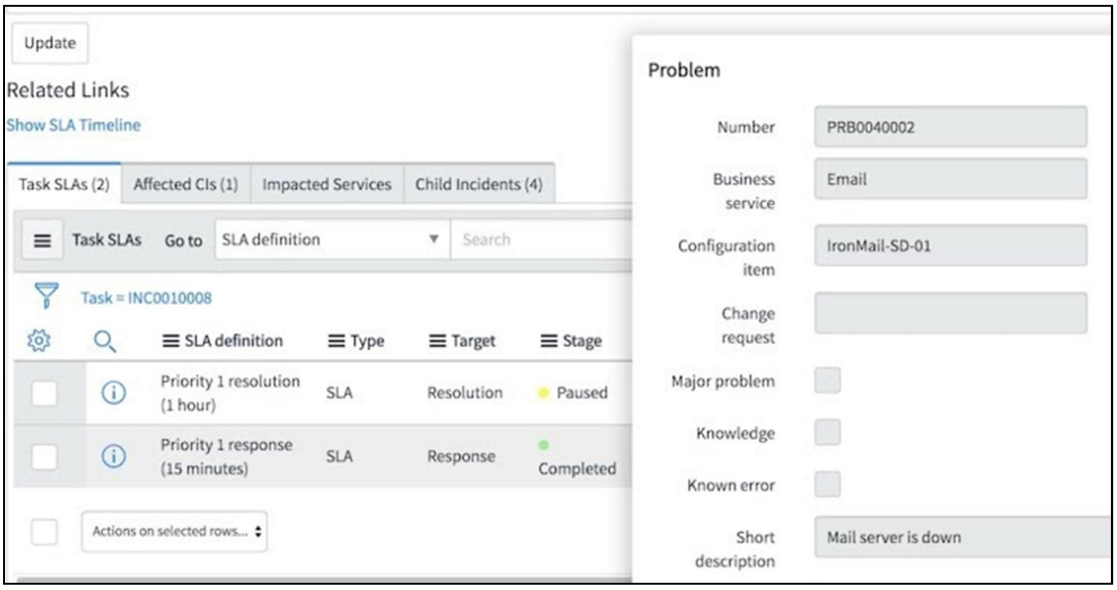

Figure 3: Screenshot results of Access Control

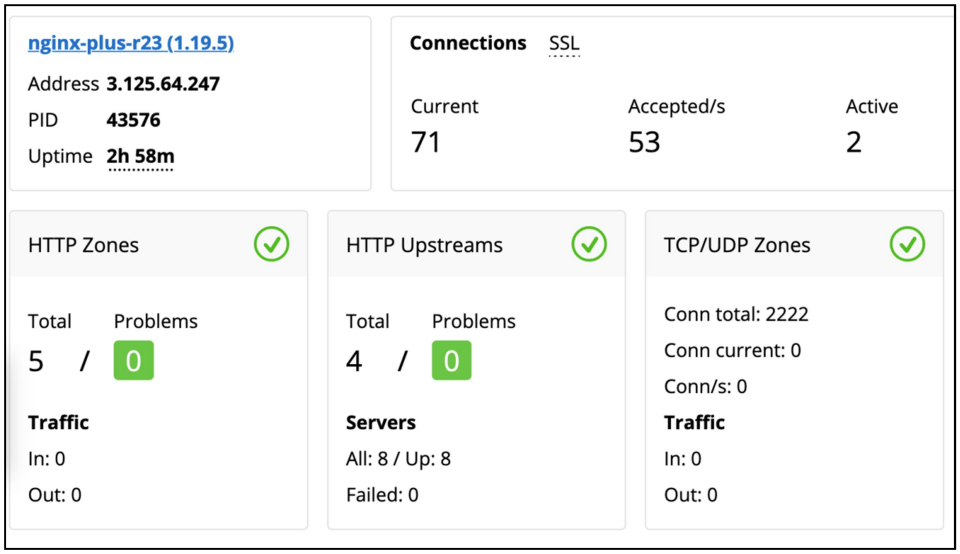

Figure 4: A status of Monitoring on the page of the admin

CONCLUSION

In this paper, we addressed the newly emerging data protection problem associated with security and privacy in the healthcare cloud scenario. We proposed a novel CASQAC model for controllability, traceability of data, and authorized access to cloud resources under a fine-grained data protection scheme. Furthermore, we also proposed and develop an AAS that is capable of tracing, tracking, and triggering an alert on operation, data, or policy violations in a health cloud environment. Current implementations are only initial prototypes as a proof-of-concept but constitute the first step towards a comprehensive solution for a novel data protection scheme in the healthcare cloud. approach can be extended to a large real cloud platform due to its distributed nature and low-couple architecture design.

REFERENCES

[1] Egala BS, Pradhan AK, Badarla VR, Mohanty SP. Fortified-chain: a blockchain based framework for security and privacy assured internet of medical things with effective access control. IEEE Internet of Things Journal. 2021 Feb 12.

[2] Rani, D. R., & Geethakumari, G. (2015, December). A meta-analysis of cloud forensic frameworks and tools. In 2015 Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG) (pp. 294-298). IEEE.

[3] Rani Radha, D., Bharati Vini, A., & Sravani, A. (2012). Analysis of Dendrogram Tree for Identifying and Visualizing trends in Multi attribute Transactional Data. International Journal of Engineering Trends and Technology, 3, 14-18.

[4] Gupta M, Sandhu R. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. InProceedings of the 23rd ACM on symposium on access control models and technologies 2018 Jun 7 (pp. 193-204).

[5] Denis R, Madhubala P. Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications. 2021 Jun; 80(14): 21165-202.

[6] Ogundokun RO, Awotunde JB, Adeniyi EA, Ayo FE. Crypto-Stegno based model for securing medical information on IOMT platform. Multimedia tools and applications. 2021 Jul 19:1-23.

[7] Tan H, Kim P, Chung I. Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for

Pandemic Control. Electronics. 2020 Oct; 9(10): 1683.

[8] Wang T, Quan Y, Shen XS, Gadekallu TR, Wang W, Dev K. A privacy-enhanced retrieval technology for the cloud-assisted Internet of Things. IEEE Transactions on Industrial Informatics. 2021 Aug 10.

[9] Chen CY, Wu HM, Wang L, Yu CM. Practical integrity preservation for data streaming in cloud-assisted healthcare sensor systems. Computer Networks. 2017 Dec 24; 129: 472-80.

[10] Ranjeeth, S., & Latchoumi, T. P. (2020). Predicting Kids Malnutrition Using Multilayer Perceptron with Stochastic Gradient Descent. Rev. d'Intelligence Artif., 34(5), 631-636.

[11] Dr.P.Sivakumar, "Exploring The Trajectory Prediction Using Lstm And Extreme Machine Learing", journal of critical reviews, issn- 2394-5125 vol 7, issue 10, 2020. (Scopus)

[12] Dr.P.Sivakumar, "Design and analysis the performance of real time content delivery network using beam scanning" journal of critical reviews, ISSN- 2394-5125 VOL 7, ISSUE 04, 2020.

[13] Venkata Pavan, M., Karnan, B., & Latchoumi, T. P. (2021). PLA-Cu reinforced composite filament: Preparation and flexural property printed at different machining conditions. Advanced Composite Materials, https://doi.org/10.1080/09243046.2021, 1918608.

[14] S Ezhilarasi, T. P., Kumar, N. S., Latchoumi, T. P., & Balayesu, N. (2021). A Secure Data Sharing Using IDSS CP-ABE in Cloud Storage. In Advances in Industrial Automation and Smart Manufacturing (pp. 1073-1085). Springer, Singapore.

[15] Shen J, Liu D, Shen J, Liu Q, Sun X. A secure cloud-assisted urban data sharing framework for ubiquitous-cities. Pervasive and mobile Computing. 2017 Oct 1; 41: 219-30.

[16] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telematics and Informatics. 2019 May 1; 38: 100-17.