University of Baghdad
College of Engineering

Journal of Engineering

journal homepage: www.joe.uobaghdad.edu.iq

Volume 29 Number 3 March 2023

An Authentication and Access Control Model for Healthcare based Cloud Services

Glena Aziz Qadir*
MSc. student
Dept. of Information System Engr.
Technical Engineering college
Erbil Polytechnic Univ.
Glena.mei20@epu.edu.iq

Bzar Khidir Hussan
Assist Prof., Ph.D.
Dept. of Information System Engr.
Technical Engineering college
Erbil Polytechnic Univ.
bzar.hussan@epu.edu.iq

ABSTRACT

Electronic Health Record (EHR) systems are used as an efficient and effective method of exchanging patients' health information with doctors and other key stakeholders in the health sector to obtain improved patient treatment decisions and diagnoses. As a result, questions regarding the security of sensitive user data are highlighted. To encourage people to move their sensitive health records to cloud networks, a secure authentication and access control mechanism that protects users' data should be established. Furthermore, authentication and access control schemes are essential in the protection of health data, as numerous responsibilities exist to ensure security and privacy in a network. So, the main goal of our suggested solution is to maintain a secure authentication and access control mechanism for health cloud data. Thus, in this work, Security Secret Key Provider (SSKP) phase is proposed for the E-healthcare-based cloud that consists of two parts. The first is an authentication scheme that is Security Secret Key (SSK) and the second is a modular access control mechanism. We explain the methodology of the proposed approach through appropriate evaluation results, which improves system security and performance by minimizing the time spent to get authentication and access the data. Simulation results indicate that our approach is significantly more effective than existing research.

Keywords: Cloud, Data security, privacy, Authentication, Access control, E-healthcare.

*Corresponding author

Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2023.03.02

Article received: 08/11/2022
Article accepted: 29/01/2023
Article published: 01/03/2023

نموذج المصادقة والتحكم في الوصول للرعاية الصحية خدمات كلاود الاساسية

گلينه عزيز قادر*
طالبة ماجستير
كلية هندسة تقنية– جامعة بوليتكنيك أربيل
اربيل –العراق

بزار خضر حسين
استاذ مساعد، دكتوراه
كلية هندسة تقنية– جامعة بوليتكنيك أربيل
اربيل – العراق

الخلاصة

تستخدم أنظمة السجلات الصحية الإلكترونية (EHR) كوسيلة فعالة لتبادل المعلومات الصحية للمريض مع الأطباء وأصحاب المصلحة الرئيسيين الآخرين في القطاع الصحي من أجل الحصول على قرارات وتشخيصات محسنة لعلاج المرضى. نتيجة لذلك ، يتم تسليط الضوء على الأسئلة المتعلقة بأمان بيانات المستخدم الحساسة. لتشجيع الأشخاص على نقل سجلاتهم الصحية الحساسة إلى الشبكات الكلاود ، يجب إنشاء آلية آمنة للمصادقة والتحكم في الوصول تحمي بيانات المستخدم. علاوة على ذلك، تعد مخططات المصادقة والتحكم في الوصول ضرورية لحماية البيانات الصحية ، حيث توجد العديد من المسؤوليات لضمان الأمن والخصوصية في الشبكة. لذا ، فإن الهدف الرئيسي من حلنا المقترح هو الحفاظ على آلية آمنة للمصادقة والتحكم في الوصول لبيانات السحابة الصحية. وبالتالي ، في هذا العمل ، تم اقتراح مرحلة مزود مفتاح الأمان السري (SSKP) للكلاود على الرعاية الصحية الإلكترونية والتي تتكون من جزأين. الأول هو نظام مصادقة وهو مفتاح الأمان السري (SSK) والثاني هو آلية التحكم في الوصول المعيارية. نوضح النهج المقترح من خلال نتائج التقييم المناسبة ، مما يحسن أمان النظام وأدائه من خلال تقليل الوقت المستغرق للحصول على المصادقة والوصول إلى البيانات. تشير نتائج المحاكاة إلى أن نهجنا أكثر فعالية بكثير من الأبحاث الحالية.

الكلمات الرئيسية: السحابة ، أمن البيانات ، الخصوصية ، المصادقة ، التحكم في الوصول ، الرعاية الصحية الإلكترونية.

1. INTRODUCTION

With the use of networks, servers, memory, software, and services such these that can be quickly provided and delivered with the least of management work and interaction from service providers, cloud computing enables quick, on-demand work access to a shared stock of customizable computational resources. The cloud guarantees availability and the five key features of the cloud are on-demand self-service, global network access, location-independent resource pooling, quick adaptability, and measurable service. It provides computing services through three delivery models which are a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), as well as three deployment models are public, private, and hybrid clouds **(Xiao and Xiao, 2012)**. Cloud computing refers to the use of internet-accessible healthcare servers to collect, monitor, and analyze healthcare data. E-Health services enable the effective communication of patient data across various entities such as nurses, doctors, laboratory staff, receptionists, and pharmacists. The data owner in E-Health prepares a content provider who may keep and share health records. The cloud computing model offers several options for enabling flexible and controllable information sharing. However, cloud authentication and access control concerns represent significant barriers to the wide adoption of cloud-based E-Health services. Data sharing between interacting entities, for example, through the cloud exacerbates security problems. Current authentication and access control systems are inappropriate for the cloud. Several approaches have been discussed to address issues of cloud security and privacy of data **(Li, et al., 2010)**. To communicate data securely and confidentially, we must handle two issues. The first is how to authenticate the users. The second question is how we may manage to access data for these users. To answer the first question, we require a secure and trustworthy authentication technique that allows us to authenticate authorized users simultaneously protecting user privacy. According to the second question, the system must give the users access according to the policies established by the system admin. Concerning the second point, typical access control techniques cannot be used in this context since they assume that servers in the same domain are completely trusted and capable of enforcing access control rules.

Due to the fact that cloud servers are placed outside of the participant's trusted zone, sensitive data must be secured from unauthorized access. It becomes more and more difficult to solve these security issues in healthcare services. The suggested method allows the hospital staff to keep their data on the cloud. In this research, we propose an SSKP layer in the E-healthcare system that allows secure authentication and modular data access control at the same time.

To verify and ensure the security and privacy of the user's data, we add a new layer of Security Secret Key Provider (SSKP) for the authentication process based on Message Authentication Code (MAC) algorithm. Users are also given flexible access rights based on their role and rights in the hospital system. Our method protects data privacy by using encryption techniques while still allowing for search over encrypted data.

2. RELATED WORKS

Addressing security and privacy issues in E-Health based cloud has been the subject of extensive research. The suggested secure E-Health system solutions are reviewed. A novel web-based system is suggested by **(Boyinbode and Toriola, 2015)** that would allow nurses, doctors, and pharmacists to access patients' medical records. The patient's information is kept on the local cloud. Remote access to it and updating the data are both possible. It is perfect for health centers where other doctors must share patient data records to collaborate on treatments. This policy's disadvantage is that the patient is not given access to their medical records.

A necessary access control mechanism is provided by Luna et al. **(Luna, et al., 2010)** to protect patient meta-data. The approach encrypts data utilizing fragmented cryptography and uses a Message Authentication Code to secure data. This model shows how fragmentation following encryption can boost overall security since it forces hackers to compromise additional data files. This work **(Bakker, et al., 1995)** suggested risk-management algorithms for the healthcare system. It focuses on healthcare management by using fuzzy logic. The security of personal health records is suggested in the paper **(Patel and Kantzavelou, 1995)**. Employing encryption to protect patient data shared with doctors, reduces complexity in key management for various record holders.

The major purpose of the paper **(Mercy and Srikanth, 2014)** is to provide a secure mechanism of resource sharing between more than one person from the organization. Security and privacy are offered, which facilitates the sharing of information amongst different types of cloud users. This paper describes an effective encryption system for encrypting papers that will be shared. The shared documents can be viewed once the individual making the request has been confirmed as valid. In **(Sharon and Manoj, 2017)**, the model of E-Healthcare, which has a vital role in society, was developed. This technology is designed to store and collect patient data while also communicating health-related information. It is also more concerned about the safety and privacy of patients. They collect real-time health and personal information from people and communicate it to healthcare providers for authorized specialists to determine the appropriate treatment. They send PHI to the cloud in the form of images and text, as well as personal problems relating to medical history. A technique that has been frequently utilized in cloud storage to minimize upload space and bandwidth capacity and remove the qualified experts' authority to decide on the appropriate action to take. MeDshare, which offers a mechanism to share medical data without compromising privacy, is discussed in **(Xia, et al., 2017)**. This model can keep an eye out for any harmful activity by keeping track of who has access to the information. This allows for the tracking of available information. Every action is documented and carried out in a proof-based manner **(Alzahrani, et al., 2020)**. Blockchain technology produced a data-sharing paradigm that is used by cloud service providers. This architecture uses smart contracts as well as a few other methods to acquire access to data, monitor the nature and behavior of information, and perform other tasks including monitoring any access violations brought on by harmful attacks. Data monitoring is made feasible using this architecture **(Kumar and Gaba, 2020)**.

(Hossain and Muhammad, 2014) worked on an innovative approach to electronic medical record storage in a cloud-based system. Shamir's Secret Sharing Mechanism is used in the recommended strategy to protect data security. The healthcare center divides the EHR into several categories. The segments are evenly divided across the cloud servers. The healthcare facility collects every segment from fragmented cloud servers whenever a legitimate user requests access to the EHR to recreate the EHR. The EHR's efficiency is increased using this technique by outsourcing all patient data, which can be recreated utilizing cloud computing. The authors assert that they have developed the innovative idea of EHR separation and recreating. The approach is a very effective and secure way to handle medical records electronically, according to theoretical and empirical analyses. The architecture is insufficient to prevent attacks and illegal resource access.

(Chenthara, et al., 2019) examined and analyzed several studies and found several issues with securing e-healthcare. EHR security, cloud architecture, and security are some of them. Additionally, the authors point out that there is still much to be learned about EHR security. Another strategy is discussed by **(Huang, et al., 2018)** and involves using cloud computing for EHR and Mobile Healthcare Social Networks to share data and connect profiles. The plan enables identity-based cryptography to be used to encrypt medical records. Additionally, this approach allows for the performance of attribute-based conditional data re-encryption. It is said that the system will protect against data monitoring. To provide a very flexible and secure authorization, it uses a profile-matching technique based on identity-based encryption and an equality test. To offer authentication, sensitivity, and other access control services in healthcare systems, a framework based on trust negotiation is presented. Using digital credentials, parties may mutually disclose attributes to carry out sensitive transactions. But the method is not sufficient to protect the E-healthcare system from all common threats. The security features of E-Healthcare systems, particularly access control techniques, were highlighted **(Singh and Chatterjee, 2017)** the authors argue that their plan outperforms other established access control methods. The level of trust between the communicating parties is the foundation of the suggested access control paradigm. Based on user behavior, the level of trust is assessed. Only when both parties' levels of trust and understanding of service and the consumer are equal to the mutual trust target value is the user request allowed. The concept, according to the author, guarantees that only reliable and trustworthy users have access to medical records. **(Van Gorp and Comuzzi, 2013)** proposed "My PHR Machine," a safe e-healthcare solution. It combines PHR with cloud-based solutions. The hospital staff and he may access, exchange, and assess PHR data using HR software. Another benefit of this strategy is that it makes it easier and more secure to access many users' data simultaneously. The cloud also provides access to the data gathered through the My PHR machine. There is no faster way to get medical records using this system.

The following are the major contributions of this study.

- The proposed model includes a secure layer called SSKP.
- A data access control mechanism based on user rights to access and use the data is used.
- simulate the results and compare them to existing research. Also, analyze the proposed framework to assess its security and the time necessary to access the data.

3. MATERIALS AND METHOD

Users in our model include physicians, secretaries, pharmacists, laboratories, and administrators, who send/receive the encrypted healthcare data in the cloud to handle the most computationally intensive tasks. To access the system the user should be authenticated through the proposed method then according to data access rights can be accessed.

Additionally, they upload searchable encrypted indexes to the cloud server, permitting keyword searches across encrypted data. During the access control procedure, only authorized users are given access to the decrypted data, the data is accessible to each user based on their role and the results of the search over the encrypted data are delivered to the user. The suggested paradigm includes three layers: the Cloud, the Security Secret Key Provider (SSKP), and the system members. **Fig. 1** shows the proposed model.

1) Cloud: The cloud provides users with infinite storage space. It provides consumers with simple and effective storage services. The cloud is a semi-trusted third party that provides data storage and download services. Users who want the same data and documents or files will join a group and upload their material to the cloud. These files may now be shared with other system members.

2) SSKP: The client can access the encrypted data using an email ID and Password as shown in **Fig. 2.** Then the key is obtained from the Security Secret Key Provider (SSKP), which is responsible for giving updates to the key. The SSKP steps are explained in **Fig. 3**.

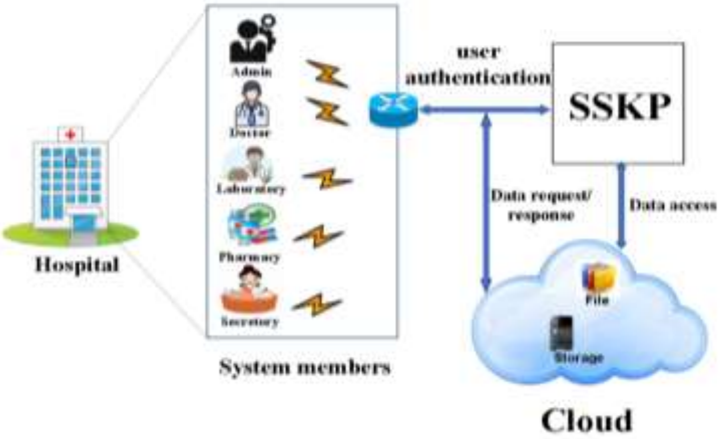
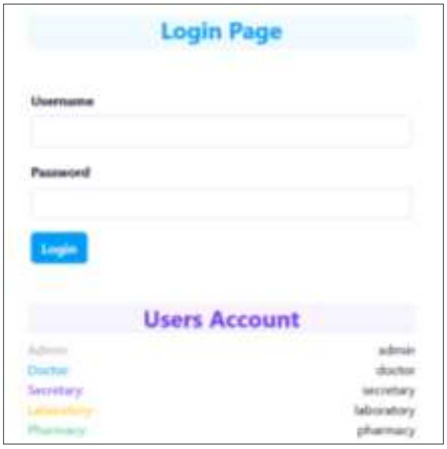


Figure 1. Added SSKP to the E-healthcare model

Users must first register their data on the website. They must select a password for the authentication procedure. After successfully registering, the user must view or access their data using their login. Once the password is entered and matched with the user's password, it asks for the Security Secret Key (SSK), steps of creating an SSK are shown in **Fig. 4.** Using key SK (0 < SK < n), SK+ is generated by padding on the left side of key SK until the length becomes n bits. n is the block size. SK+ is EXORed with iPad and the result is X1. We have to append X1 with Token Code (TC). After appending X1 to TC we have to apply HASH-256. Simultaneously we have to apply the initialization vector (IV) which is a buffer of size m-bits. The result produced is therefore the number of blocks (m)-bit hash code. Similarly, m-bits are padded to n-bits and SK+ is EXORed with iPad producing output X2 bits. X2 is appended to the n-bits and once again hash function is applied with IV to the block. This further results in an m-bit hash code. Then it takes the hash code low-order 4 bits and uses them as a byte index *I* after that selects 4 bytes starting at byte index *i.* After generating the SSK by the SSKP layer it has to send to the user by email ID. After the user accessed the sent SSK the system authenticates the user so can log in and can access the data according to the user's role.

3) System members: The users who wish to share the data by identifying their password and the SSK, which helps in getting authentication and accessing data for sharing. Fault tolerance is performed to enhance the system's efficiency.



Admin	admin
Doctor	doctor
Secretary	secretary
Laboratory	laboratory
Pharmacy	pharmacy

Figure 2. The login page

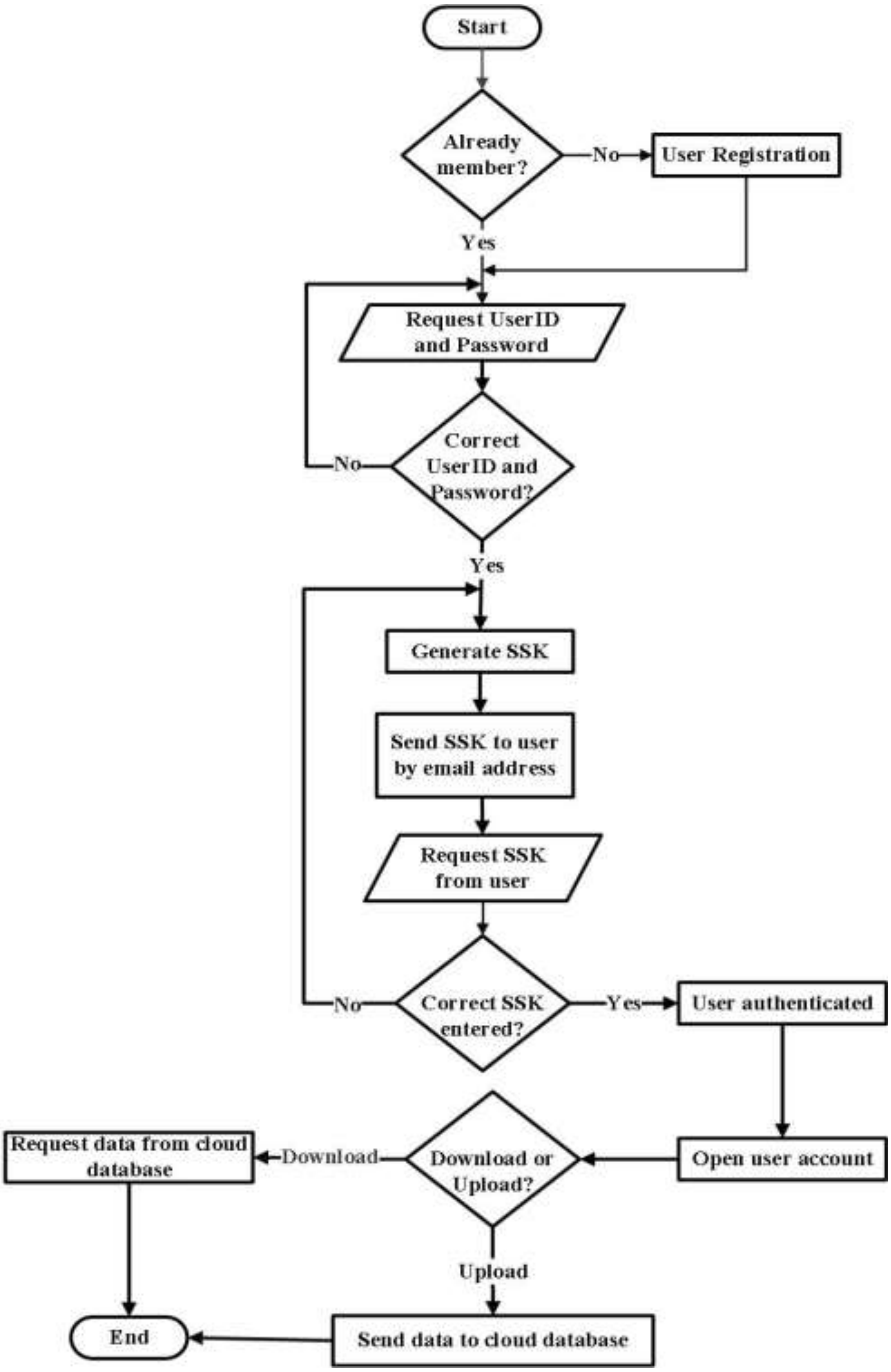


Figure 3. The system working

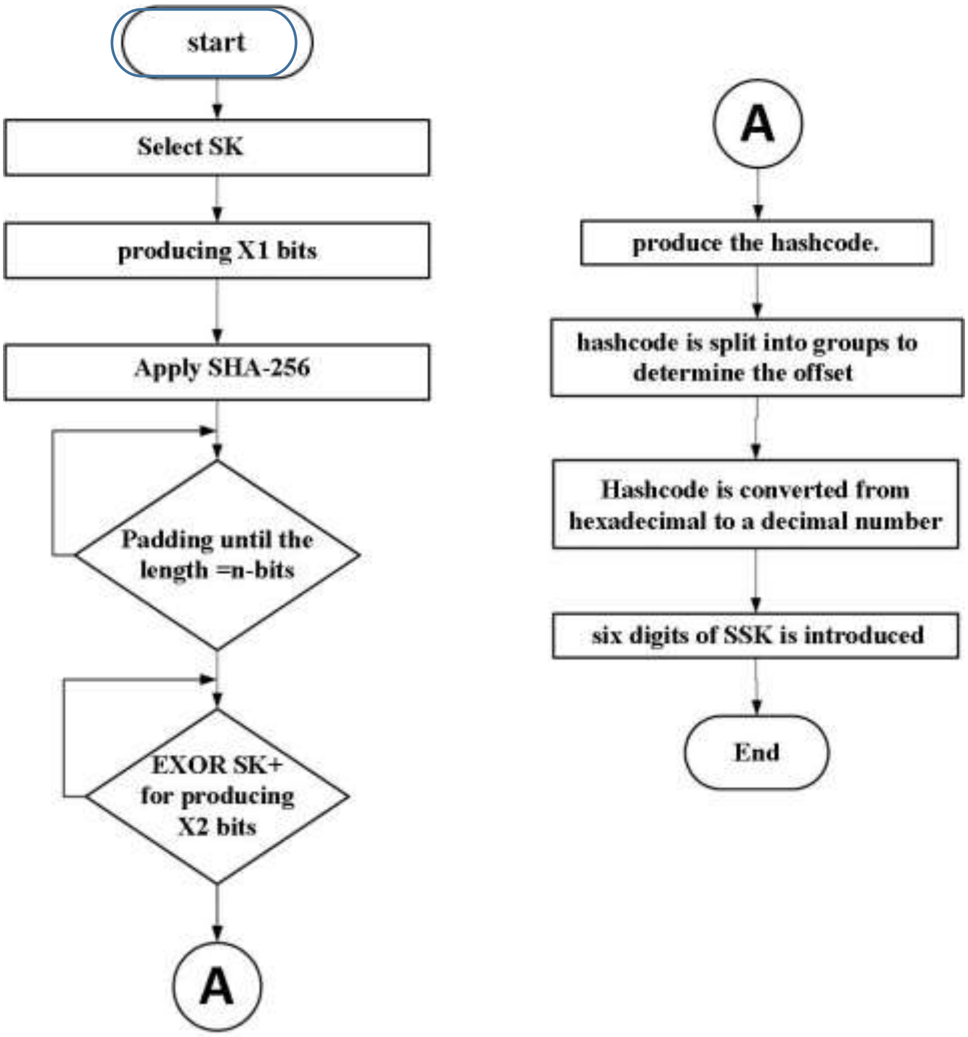
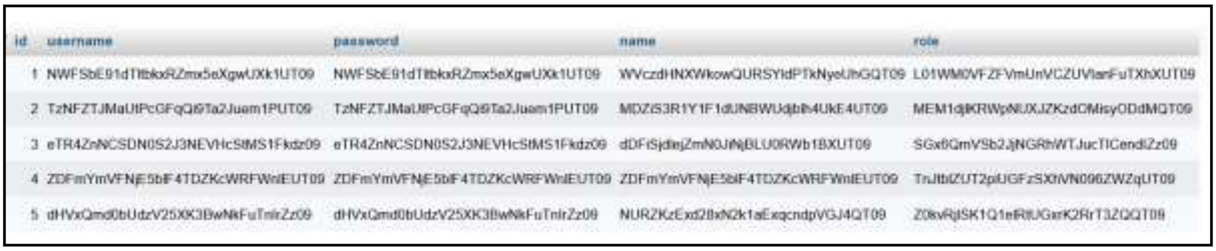

start
Select SK
producing X1 bits
Apply SHA-256
Padding until the length =n-bits
EXOR SK+ for producing X2 bits
A
A
produce the hashcode.
hashcode is split into groups to determine the offset
Hashcode is converted from hexadecimal to a decimal number
six digits of SSK is introduced
End

Figure 4. Generating SSK

In our E-health system, the role-based access control (RBAC) approach provides efficient security and flexibility. The RBAC is perfect for the E-health paradigm. The RBAC approach splits all users into some categories in our framework: administrator, doctor, laboratories, recipients, and pharmacist. We set up the various related permissions and actions in the basic frame based on the varied requirements of each role. We will discuss the user roles below:

Admin is a hospital IT manager who can effectively register the hospital system with the cloud. Using a personal email ID and password, the administrator connects securely with the cloud via the gateway. To access the data, the admin must insert the SSK that was delivered to the email address. Patients' data are kept in the database system according to the standards established by the hospital IT admin, and the security system provides secure access to the Cloud. According to the end-to-end encryption concepts, the database is encrypted using the AES and SHA algorithms with a secret key **Fig. 5** is the result of the encryption method for protecting the database from hackers, in case they get access to the database, they will get nothing from this hashing records.



id	username	password	name	role
1	NWFSbE91dTltbkxRZmx5eXgwUXk1UT09	NWFSbE91dTltbkxRZmx5eXgwUXk1UT09	WVczdHNXWkowQURSYldPTkNyeUhGQT09	L01WM0VFZFVmUnVCZUVlanFuTXhXUT09
2	TzNFZTJMaUtPcGFqQi9Ta2Juem1PUT09	TzNFZTJMaUtPcGFqQi9Ta2Juem1PUT09	MDZiS3R1Y1F1dUNBWUdjbllh4UkE4UT09	MEM1djlKRWpNUXJZKzdOMisyODdMQT09
3	eTR4ZnNCSDN0S2J3NEVHcStMS1Fkdz09	eTR4ZnNCSDN0S2J3NEVHcStMS1Fkdz09	dDFiSjdlejZmN0JiNjBLU0RWb1BXUT09	SGx6QmVSb2JjNGRhWTJucTlCendlZz09
4	ZDFmYmVFNjE5blF4TDZKcWRFWnlEUT09	ZDFmYmVFNjE5blF4TDZKcWRFWnlEUT09	ZDFmYmVFNjE5blF4TDZKcWRFWnlEUT09	TnJtblZUT2plUGFzSXhVN096ZWZqUT09
5	dHVxQmd0bUdzV25XK3BwNkFuTnlrZz09	dHVxQmd0bUdzV25XK3BwNkFuTnlrZz09	NURZKzExd28xN2k1aExqcndpVGJ4QT09	Z0kvRjlSK1Q1elRlUGxrK2RrT3ZQQT09

Figure 5. The encrypted database

A doctor is a person who looks after the patients who have been committed to him for treatment. Only the connected doctor should typically have access to the patient’s information. The doctor uploads all of the patient data and encrypts it before storing it in the cloud database. The patient is the person who has been referred to the hospital for treatment or a checkup. Based on his diagnosis, he is assigned a certain doctor. In addition, the patient provides a unique identifying number. After the doctor saw the patient, the patient’s information is sent to the laboratory or pharmacy. The Laboratories can see the information of the patient and send back the results of the tests to the doctor. Then the drugs for the patient are sent to the pharmacy. The pharmacist can see the information report of the patient that contains the drugs written to the patient by the doctor. At the end of all the check-ups in the hospital and consulting with a doctor, a patient is provided a medical report and stored in the cloud database.

4. RESULTS AND DISCUSSION

The performance of the proposed model is evaluated in this section. The time cost comparison is performed to determine the spend time for authenticating users and accessing data according to the design, as the number of participants increases, the time increase. The computation cost for several participants in the authentication stage is determined, and the efficiency of our approach is compared. When there are seven users n=7, the time cost for calculation in our technique is 0.05 in the authentication phase shown in **Fig. 6.**
The time cost of our method is gradually increasing in this step when the number of users is 993. To evaluate the performance of our system accessing data for multiple users. The typical response time for accessing data for multiple users is shown in **Fig. 7**. The results of the experiment show that our system is capable of responding to a lot of users in a reasonable response time. We have 300 users requesting 153 bytes of data from the homepage at the same time the time spend is 3.8 milliseconds, today patient the needed time is 3 milliseconds, for All patients data we need 3.2 milliseconds, and 3.1 milliseconds for new patient page data. The responding time gradually increases for all the databases. Also, we obtain the response time for 1000 participants requesting the same data for the homepage 5.5 milliseconds are needed, 5.2 milliseconds are needed for today's patient, time spent for all patient data 4.9 milliseconds, and 5 milliseconds for a new patient.

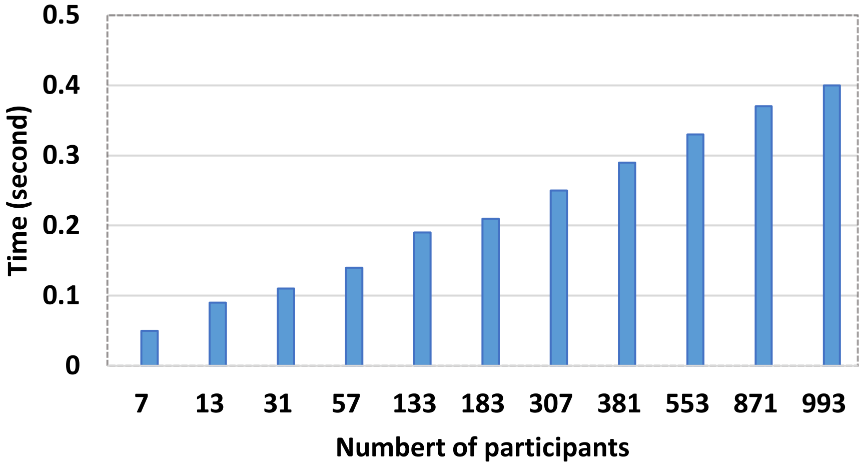


Figure 6. Authentication phase

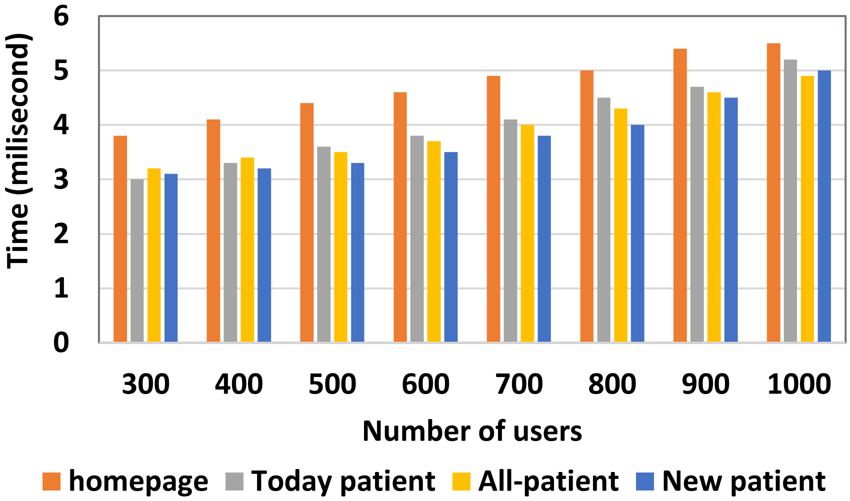


Figure 7. Performance evaluation

5. CONCLUSIONS

In this paper, we propose a new method for achieving authentication and modular access control at the same time. In our model, the data owner has a set of health records to publish and store on cloud servers. Encrypted data using encryption and hashing algorithms are stored in the cloud to protect user data from malicious users. Valid users are authenticated through the authentication process, which is based on an SSKP. The access control method determines which users have access to which data. The proposed method is in control of authentication and access control management. The simulation results indicate that our scheme achieves a good performance.

REFERENCES

Alzahrani, A. G. M., Alenezi, A., Mershed, A., Atlam, H., Mousa, F., and Wills, G. 2020. A framework for data sharing between healthcare providers using blockchain. *In Proceedings of the 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020)*, pp. 349-358. doi:10.5220/0009413403490358

Bakker, R., Barber, B., Tervo-Pellikka, R., and Treacher, A., 1995, Communicating health information in an insecure world. *In Proceedings of the Helsinki Working Conference*, 43 (1),p. 2.

Boyinbode, O., and Toriola, G., 2015. CloudeMR: a cloud based electronic medical record system. *International Journal of Hybrid Information Technology,* 8(4), pp. 201-212. doi:10.14257/ijhit.2015.8.4.23

Chenthara, S., Ahmed, K., Wang, H., and Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access,7, pp. 74361-74382. doi: 10.1109/ACCESS.2019.2919982

Hossain, M. S., and Muhammad, G. 2014. Cloud-based collaborative media service framework for healthcare. *International Journal of Distributed Sensor Networks,* 10 (3), p. 858712. doi:10.1155/2014/858712

Huang, Q., Yue, W., He, Y., and Yang, Y. 2018. Secure identity-based data sharing and profile matching for mobile healthcare social n*etworks in cloud computing. I EEE Access, 6, pp. 36584-36594. doi: 10.1109/ACCESS.2018.2852784*

Kumar, P., and Gaba, G. S. 2020. Biometric-based robust access control model for industrial internet of things applications. *IoT Security: Advances in Authentication*, pp. 133-142. doi:10.1002/9781119527978

Li, M., Yu, S., Ren, K., and Lou, W., 2010. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *Security and Privacy in Communication Networks: 6th International ICST Conference, SecureComm 2010, Singapore, September 7-9, 2010. Proceedings 6*, pp. 89-106. doi:10.1007/978-3-642-16161-2_6

Luna, J., Dikaiakos, M., Marazakis, M., and Kyprianou, T. 2010. Data-centric privacy protocol for intensive care grids. *IEEE Transactions on Information Technology in Biomedicine*, *14*(6), pp. 1327-1337. doi: 10.1109/TITB.2010.2073478

Mercy, S.S., and Srikanth, G.U., 2014. An efficient data security system for group data sharing in cloud system environment. *International Conference on Information Communication and Embedded Systems (ICICES2014)*, IEEE, pp. 1-4. doi: 10.1109/ICICES.2014.7033956

Patel, A., and Kantzavelou 1995. Implementing network security guidelines in health care information systems. *Medinfo. MEDINFO*, *8*, pp. 671-674.

Sharon, R.S., and Manoj, R.J., 2017. E-health care data sharing into the cloud based on deduplication and file hierarchical encryption. *International Conference on Information Communication and Embedded Systems (ICICES), IEEE,* pp. 1-6. doi: 10.1109/ICICES.2017.8070739

Singh, A., and Chatterjee, K. 2017. A mutual trust based access control framework for securing electronic healthcare system. 14th IEEE India Council International Conference (INDICON). IEEE, pp. 1-6. doi: 10.1109/INDICON.2017.8487658

Van Gorp, P., and Comuzzi, M. 2013. Lifelong personal health data and application software via virtual machines in the cloud. *IEEE Journal of biomedical and health informatics*, *18*(1), pp. 36-45. doi: 10.1109/JBHI.2013.2257821

Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., and Guizani, M., 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access*, *5*, pp. 14757-14767. doi: 10.1109/ACCESS.2017.2730843

Xiao, Z., and Xiao, Y., 2012. Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, *15*(2), pp. 843-859. doi: 10.1109/SURV.2012.060912.00182