

Enhanced Secure Cloud-Based e-Health System Using Three Tier Security and Authentication Levels

¹Ogwo Eme, ²Oti Joyce Ifeoma, ³Inya Ogonnia Umeh and ⁴Chukwuma Sopuruchi Egwu

^{1,2,3,4} Department of Computer Science,
Akanu Ibiam Federal Polytechnic, Unwana, Nigeria

²joyce_oti@yahoo.com, ³inyaogonniaume@gmail.com, ⁴sopuruchiibiam@gmail.com

Corresponding Author: ¹ogwoeme22@gmail.com

Abstract

The deployment of digital technologies such as ICT and cloud computing is emerging as one of the most rapidly growing areas in healthcare today. Security concern is one of the main challenges that deter many healthcare providers in the fast adoption of cloud computing technology in providing reliable and efficient healthcare services to their patients. We therefore propose an Enhanced Secured Cloud based e-Health System that uses three levels of security and three levels of Authentication to ensure that only authorized users have access to the system and preserve the privacy of patients' electronic health records stored in the Enhanced Secure Cloud Based e-Health System. These security mechanisms were integrated in the proposed system so that it can provide means of ensuring that only authorised persons have access to the Enhanced Secure Cloud Based e-Health System. It also ensures that the integrity of patients' health records stored in the e-Health System is not compromised.

KEYWORDS: Access Control, Authentication, Cloud Computing, Digital Technologies, e- Health System, Hashing Passwords, Security Levels, Two-Factor Authentication (2FA) Technique

1. INTRODUCTION

Healthcare is one of the fundamental human rights in any nation. People have to go to the public healthcare institutions or private medical centres for medical check-up and treatments. The emergence of Information and Communication Technology has gone a long way in bridging the gap of interaction between healthcare givers and patients that visits the hospital for their health care services. Adoption of Information and Communication Technology (ICT) with the healthcare system is a demand of this day for increasing the efficiency of medical information management (Sharma, 2011).

The deployment of Information and Communication Technology has impacted greatly on the development and advancement of all sectors of our society. It has always been intertwined with human development for even every small economic or social growth. Information and Communication Technology (ICT) and web services have a major impact on the quality of services and peoples' lifestyle. The implementation of ICT in the health sector, popularly known as e-Health, is emerging as one of the most rapidly growing areas in healthcare today (Srivastava et. al, 2015). At the same time it also helps in imparting knowledge and creating interest among common people. These applications are simple, easy to use, engaging, and capable of delivering relevant information for healthcare services to diverse users.

The patients' electronic medical records are available to healthcare providers through the help of Cloud computing by ensuring that these records are available when they are needed especially in emergency situations. Current trends aim towards accessing information anytime, anywhere and this can be achieved by moving healthcare information to the cloud. Most healthcare institutions are now shifting the burden of managing and maintaining complex Health Information Technology (HIT) to the Cloud service providers (Teng et al, 2010). The adoption for Cloud computing in healthcare also provides the health care institutions the ability to exchange data between dissimilar and separate systems. Also cloud computing can serve as an education tool for providing healthcare professionals the needed medical knowledge on health related issues (Nagy, 2005). Also stakeholders involve in the provision of healthcare including doctors, nurses and other healthcare providers can gain access to private cloud through the cloud infrastructure of a particular Cloud Service Provider (CSP) and are able to view information such as the medical history of their patients before attending to them (Yaw et al, 2015).

Walters (2021) broadly defines e-Health as "the use of technology and specifically electronic communication within healthcare environments." e-Health is the delivery of healthcare using modern electronic information and communication technologies when healthcare providers and patients are not directly in contact and their interaction is mediated by electronic means. Among other things, the services that are thus provided include physical and psychological diagnosis and treatment, telepathology, vital signs monitoring, electronic prescribing, teleconsultation, etc. This approach to healthcare is increasingly being employed in geographically extended areas where the availability of healthcare is severely reduced or even non-existent, and when appropriately qualified medical personnel are available only in a centralized location (Kluge, 2020). Despite its various advantages offered by deploying health services in the cloud, there are security and privacy challenges that urgently deserve utmost attention for realization of its efficient and full scale utilization (Li et.al, 2012). As a result various security measures are being used for protecting data for these e- health systems in the cloud.

Many hospitals in Nigeria are faced with some challenges in their efforts to offer efficient healthcare services to various categories of patients who has adopted cloud based e-Health System as a tool for method of offering efficient healthcare services to their patients. Some of the challenges facing these hospitals in Nigeria that has deployed cloud based e-Health system include:

- i. Patients' health records stored in the hospitals are prone to privacy and security concerns where unauthorized persons may likely have access to patients' health records because of the manner patients' health records are presently kept in the hospitals. There is need to effect a more secure means of securing the patients' health records to ensure that only authorized persons can access these health records.
- ii. Patients who are registered with National Health Insurance Authority (NHIA) in Nigeria experience delay in accessing healthcare services in other NHIA registered hospitals especially if it is not the hospital they are originally registered to access healthcare services in Nigeria. It takes at least 24 hours to access the required authorization code for the patients to be attended to when they visit other NHIA registered hospitals different from the primary NHIA registered hospital.

These problems were noted after a careful analysis of the data collected from the hospitals and medical centres using observation and interview data collection methods and from the result of the reviewed related literature. This analysis of the data collected from the case studies show that there is need to design and implement an Enhanced Secure Cloud based e-Health System for hospitals to aid these hospitals in the provision of efficient healthcare services to patients who visit the hospitals for their healthcare needs. Therefore a carefully designed Enhanced Secure e-Health System needs to be put in place in to guarantee the security of patients' health records and users of the e- health system; and ease the way healthcare services are provided in these hospitals. From the reviewed literature, we also discovered that most of the solutions focused mainly on the security and privacy of patients. It is important that all the privacy of all users of the cloud based e-health system should be incorporated in the new system.

Based on the high need for efficient healthcare practice that has the ability to alleviate the enumerated challenges, we proposed an Enhanced Secure Cloud based e-Health System that uses three tier levels of security as proffered solution to the problems identified in many Nigerian hospitals especially as it have to do with security of patients' health records and delivery of efficient health services to patients.



To solve the issue of delay of authorisation codes needed to access NHIA healthcare centres and hospitals, the new system will be connected to NHIA via an Application A Programme Interface (API) such that the hospitals gets the required authorisation without waiting for the authorisation codes which may affect prompt health attention for treatment. The new security system will benefit Nigerian hospitals by ensuring that the beneficiaries of this insurance health scheme will continue to patronise the NHIA accredited hospitals knowing fully well that their data are secured and that health records cannot be accessed by unauthorized persons.

1.2 Related Works

Al-Anzi et al (2014) suggested a security model for Cloud Computing comprising governance, risk management and compliance. According to the authors, Cloud Computing security requirements vary quite significantly from traditional environments because services; IaaS, PaaS and SaaS. The authors recommended that an organisation should implement a framework for effective risk management and measure the performance of the risk management by metrics.

Yaw et. al (2015), proposed a cloud computing framework for e-Health adoption by Ghana Health service (GHS). Within the framework for a Cloud Based e-Health for GHS, a stakeholder in healthcare institutions including Doctors, Nurses and Physicians gain access to the GHS Private cloud through the cloud infrastructure of a particular Cloud Service Provider (CSP) and are able to view information such as the medical history of their patients before attending to them. Patients and staffs of GHS and the various hospitals are also able to use mobile devices to gain access to the GHS private cloud. The authors proposed different access control levels such as Private, Community and Public levels for accessing different types of healthcare services being rendered by GHS within the GHS private cloud service model safely by the CSP.

Sharma & Balamurugan (2020) proposed a system to implement Electronic Health Records using block-chain technology and make Electronic Health Records more secure and private. Their proposed block-chain technology keeps control over access to information using its cryptographic techniques and decentralization. It also maintained the balance between data privacy and data accessibility. The main objective of this project is the framing of data privacy and security issues in electronic healthcare.

Yang et al (2021) proposed blockchain-based architecture for Electronic Health Record (EHR) systems. It was built on top of existing databases maintained by health providers, the architecture implements a block-chain solution to ensure the integrity of data records and improve interoperability of the systems through tracking all events that happen to the data in the databases. They also introduce a new incentive mechanism for the creation of new blocks on the block-chain. Their proposed architecture is independent of any specific block-chain platforms and open to further extensions.

Chelladurai & Pandian (2022) proposed a block-chain smart contracts system designed to provide a regulated solution to the need of patients, physicians, and health service providers. Their proposed system aims to exchange health information on a block-chain platform to build a smart e-health system. Their system uses block-chain as a clinical data repository that provides patients a complete, distributed ledger record containing records of all the events and seamless access to their electronic health records through healthcare providers. As an important feature, this system provides high security and integrity through cryptographic hash functions. Their system ensure for secure storage and rapid access of health records and health information exchange between different providers, and viewership contracts on the peer to peer block-chain network.

2. METHODOLOGY AND SYSTEM DESIGN

In this research work we adopted the Object Oriented Analysis and Design Methodology (OOADM) for the design and implementation of our Enhanced Secure Cloud based e- Health System. The model for the Enhanced Secure Cloud based e- Health System is shown in Fig.3. The design of the model is illustrated using a Use Case as shown in Fig.1. This use case diagram shows how the different actors (users) interact with the system while performing their different functions based on their different role access granted to them. The login process of the use case provides the gateway to gain access to the system. The use case for this model displays all the functionalities containing all users of the secure cloud-based e-health system such as medical staff and the patients. This Use Case is designed to show the relationships between medical staff and the Cloud-based portal for the secure cloud based e-health system.



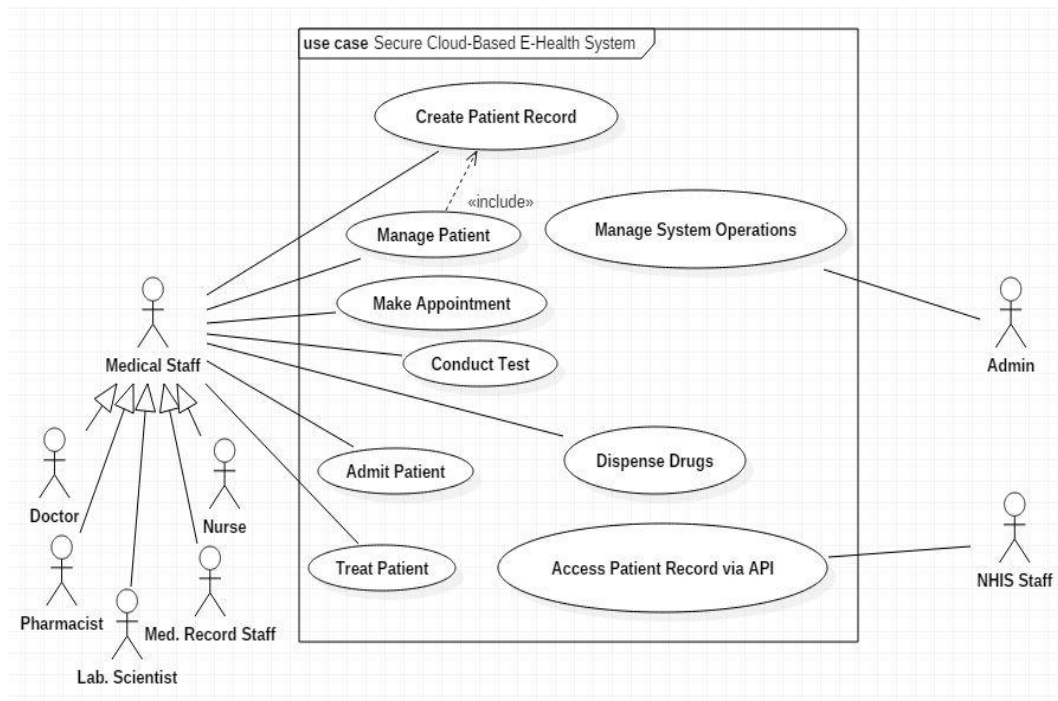


Fig. 1: System Administrator Use case

This work followed existing work as reported by Abayomi-Alli (2014) on a Cloud-based healthcare model in the delivery of healthcare services but with an enhancement on the security measures deployed for users of cloud based health system. The adopted model allows patients and healthcare staff such as doctors, nurses and pharmacists to have access to healthcare records through online websites. The advantages in using the adopted model include reducing the patients’ waiting time and offering quick and efficient healthcare delivery to the patients.

2.1 System Design

The Enhanced Cloud e-Health System consists of two major components which are: the cloud-based system and the e-health web portal. The Enhanced Secure Cloud - based System consists of a Cloud Central Database Server and the e-health web portal which provides a link for all users of the e-health access the cloud –based system through a secure web portal. The cloud Central Database acts as the unified data bank for storing of patients medical records for users of the cloud based e-health system and for the hospitals that are registered with the National Health Insurance Authority (NHIA) which can be accessed via Application Programming Interface. Through a secure Application Programming Interface (API), the cloud based e-health service system is connected to other health providers that are registered with the National Health Insurance Authority (NHIA) for sharing of patients’ electronic health records in these health institutions for the provision of healthcare services for patients who visit these NHIA hospitals. The Enhanced Secure Cloud e-Health System was implemented as a two tier application: front-end and back- end. Our enhanced Secure.

Cloud Based e -Health System Model is illustrated in Fig. 2.

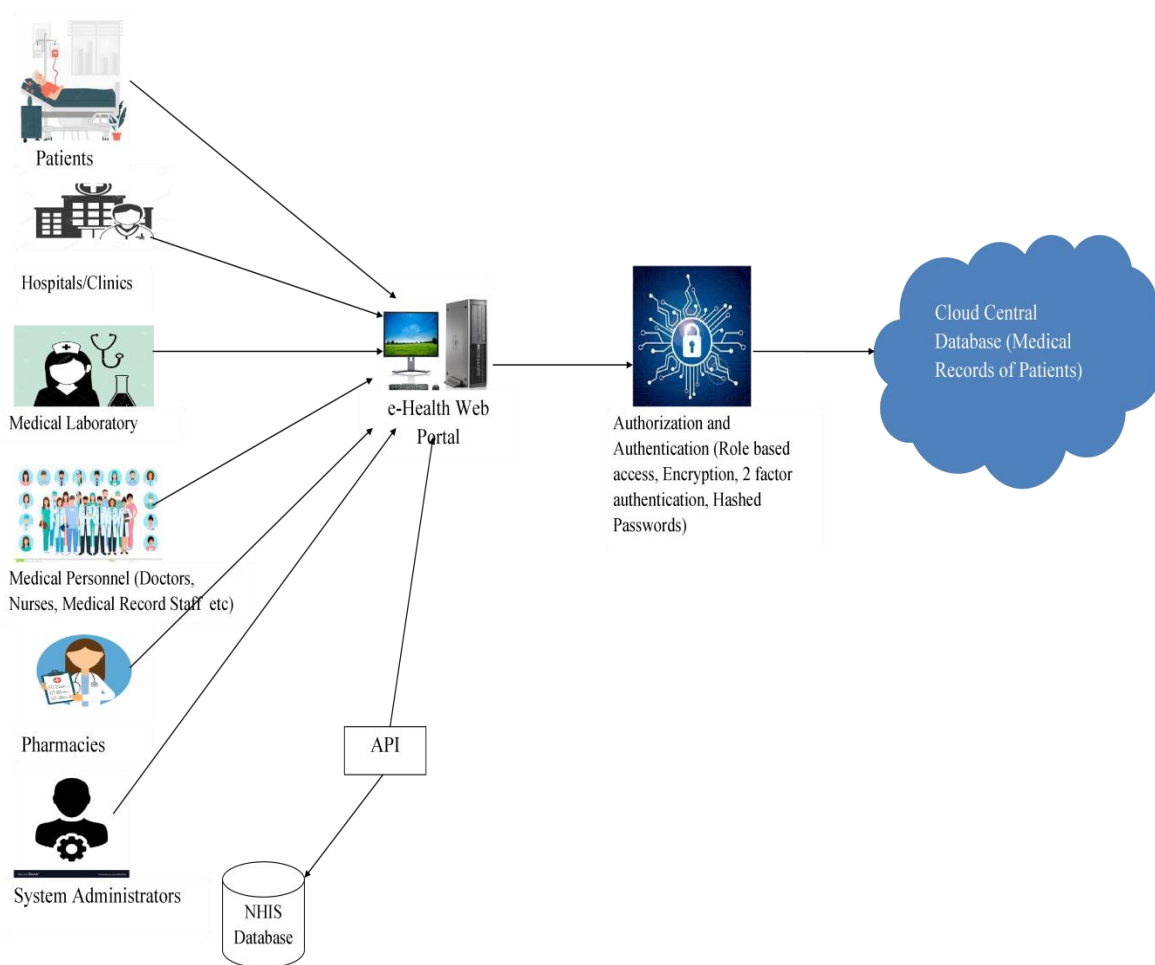


Fig. 2: The Secure Cloud Based e -Health System Model

2.2 Security Design

The two major security measures were deployed were further grouped into two major parts namely Security Levels and Authentication Levels Two forms of security measures were incorporated into the system to ensure that privacy of users of the implemented system were preserved and prevent unauthorized access to the e-health system. The two major security measures were further grouped into three tier security levels each. The two major security measures were Security Levels and Authentication Levels: The Security Levels were Data Entry Level, Access Level and Storage Level. To authenticate a user of the cloud based e-health system, three levels of authentication were also employed. The authentication levels were Two-Factor Authentication Technique, Role-based Access Control and Hashing based passwords. These measures ensure that the privacy of the entire patients’ data were maintained and safe guard the data of the different categories of users of the e-health system, and the medical records of patients against unauthorized and malicious access.

2.2.1 Security Levels

In order to ensure the security of the new system, three tier levels of security was deployed to enhance the security of the cloud based e-Health System. The system security levels are discussed as follows:

i. Data Entry Level (Data Encryption)

At this level, some parts of the data are encrypted at the point of entry to safe guard the data and maintain the privacy of the patients’ medical records. This is done to ensure that only the authorized users can have access to them at the point of access. All sensitive patient information was securely stored in a private medical record so that medical information can be shared by different doctors or medical personnel. In order to secure this transaction, the information was properly encrypted and controlled.

ii. Access Control Level

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to organization's data. Access control identifies users by verifying various login credentials, which can include usernames and passwords, PINs, biometric scans, and security tokens. Access control is a selective restriction of access to data. It consists of two main components: authentication and authorization. Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensure appropriate control access levels are granted to users. Access control was implemented as a crucial component of web application security to ensure that only the right users have the right level of access to the right resources. The user must be authenticated and authorize by the system before it can have access to the e-Health system. At the access level, Role-based access control was implemented. A user of the cloud based e-health system can only have access to the e-health system based on his role.

iii. Storage Level

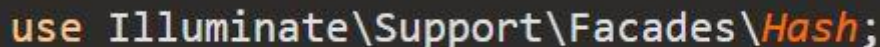
Cloud data security usually involves a number of tools, technologies, and approaches. A major advantage of the cloud is that many security features are already built into the cloud systems. This usually includes strong encryption at rest and in motion. The users' data are secure using the security features of the cloud service provider - Amazon Web Services. Amazon Web Services, the Cloud Service Provider used in this research work has a robust security features in their storage systems. Their cloud solutions are more secure than on-premises systems, hence the choice for using it for storage of data. This is done to ensure that the best data security principles of confidentiality, integrity, and availability are achieved.

2.2.2 Authentication Level

To ensure that only the authorized users have access to the cloud based e-health system, three levels of authentication were also deployed. The authentication levels were Two - Factor Authentication Technique, Role-based Access Control and Hashing based passwords. These levels of authentication are discussed as follows:

i. Hashing Based Passwords

In order to enhance the security of the e-health service system, the passwords created were hashed. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to validate the integrity of the content by detecting all modifications and thereafter changes to a hash output. The passwords created for the users of the e-health system were stored in the form of hashes so that even if the database is breached, the plaintext passwords are not accessible. This is so because a good hash function uses a one-way hashing algorithm and so the hash value or key cannot be converted back into the original key. The Hash class which encrypts characters into complex alphanumeric character was used to ensure that passwords entered by the user of the system were not intercepted or guessed by malicious users. In combination with the hash façade, bcrypt() algorithm was also adopted in some part of the system as both hashing algorithms use the same method of irreversible hashing algorithm. Figs.3, 4 and 5 show where they were used and the effect of the algorithm on characters when entered as passwords. The Hash class in Fig.3 uses the make() method to encrypt the password. The bycrpt() is function that hashes any given value against the bycrypt algorithm.



```
use Illuminate\Support\Facades\Hash;
```

Fig. 3: The Hash façade

```
protected function create(array $data)
{
    return User::create([
        'name' => $data['name'],
        'email' => $data['email'],
        'password' => Hash::make($data['password']),
    ]);
}
```

Fig. 4: Use of Hashing in encrypting password

```
$user->password = bcrypt($request->password);
```

Fig. 5: The bcrypt Implementation

ii. Two-Factor Authentication (2FA) Technique

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves. 2FA is implemented to better protect both a user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically, a password or passcode. Two-factor authentication methods rely on a user providing a password as the first factor and a second, different factor -- usually either a security token or a biometric factor, such as a fingerprint or facial scan. Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check (Loshin, 2021). The Two-factor authentication (2FA) technique was implemented in the Enhanced Secure Cloud Based e-Health System to provide a higher level of security for the patients e-health records and to ensure that only authorised and authenticated users have access the Cloud based e-Health system.

iii. Role-based Access Control Level

Role-based access control mechanism is another security measure implemented to ensure the security of the cloud based e-health service system. Each authorised user of the system is granted certain access rights to the system. In using the role - based access control mechanism, access right is granted to authenticated and authorised users on the type of relations he can perform on the system and what records he can access based on individuals or groups defined business functions. For example, a patient can only access his medical record but cannot alter any part of the record while a doctor has the access right to update the patient's record when the patient visits the hospital for his medical needs. The update includes the patient's vital signs, his drug prescription and other medical treatments given to the patient on his visit to the hospital. In ensuring that users of the system are assigned to their appropriate role, the role id was used to attach to individual user on the system. This means that every user has a role id as demonstrated in the Fig.6 and Fig.7.

From Fig.6, it can be observed that by matching the role_id from the users table (Fig.7) with the id from the roles table, the users with their roles will be easily identified. With this role-based system, the patients' privacy is relatively guaranteed. Fig. 8 illustrates the different roles that in e-Health Cloud and the different ways they will have access to.



id	name	created_at	updated_at
1	Admin	2020-04-08 08:0...	2020-04-08 08:0...
2	Doctor	2020-04-08 08:0...	2020-04-08 08:0...
3	Nurse	2020-04-08 08:0...	2020-04-08 08:0...
4	Pharmacist	2020-04-08 08:0...	2020-04-08 08:0...
5	Med. Record Staff	2020-04-08 08:0...	2020-04-08 08:0...
6	Lab. Scientist	2020-04-08 08:0...	2020-04-08 08:0...
7	Patient	2020-04-08 08:0...	2020-04-08 08:0...
* NULL	NULL	NULL	NULL

Fig. 6: Role Data Structure

gender	email_verified_at	password	userimage	role_id	department_id	isactive	rem
Male	NULL	\$2y\$10\$U4TVon...	defaultuserimage....	1	1	1	NULL
Male	NULL	\$2y\$10\$56LZlsyl...	defaultuserimage....	1	1	1	NULL
Male	NULL	\$2y\$10\$3r6onH9...	defaultuserimage....	2	3	1	NULL
Male	NULL	\$2y\$10\$wegHG...	defaultuserimage....	7	4	1	NULL
Male	NULL	\$2y\$10\$cnTtT4u...	defaultuserimage....	7	4	1	NULL
Female	NULL	\$2y\$10\$Y7c8.op...	defaultuserimage....	3	2	1	NULL
Male	NULL	\$2y\$10\$uDtmGZ...	defaultuserimage....	2	3	1	NULL
Male	NULL	\$2y\$10\$ZsgnV9x...	defaultuserimage....	4	7	1	NULL
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Fig. 7: Users Data Structure



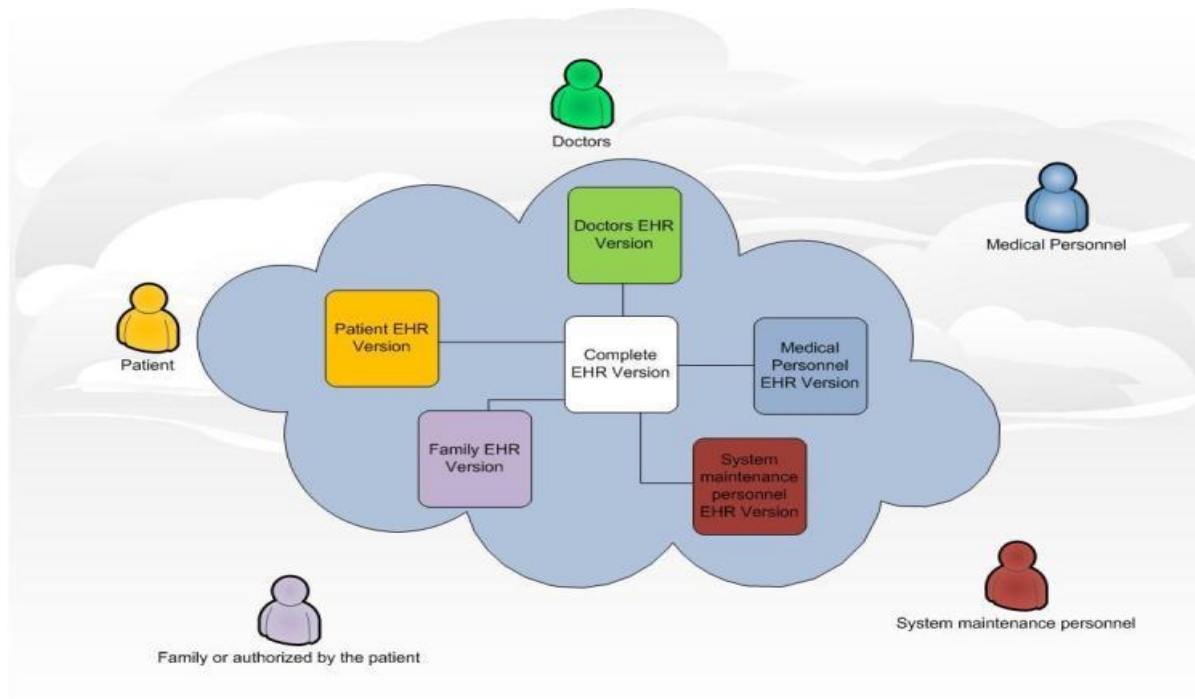


Fig. 8: Role based Users in cloud e- Health System (Rodrigues et al, 2013)

3. CONCLUSION

Security concern is one of the main challenges that deter many healthcare providers in the fast adoption of cloud computing technology in providing healthcare services to their patients. We proposed an Enhanced Secure Cloud based e-Health System that uses three tier levels of security to ensure that only authorized users have access to the system and ensures that the privacy of patients' health records are preserved. The new system was implemented using three tier security levels namely Data Entry, Access Control and Storage levels. While The Authentication levels deployed for the Enhanced Cloud Based e-Health System were Hashing based Password, Two Factor Authentication Technique and Role-based Access Control. These security measures were incorporated in the cloud based system to ensure the security of patients' electronic health records stored in the cloud. The paper "Enhanced Secure Cloud based e-Health System Three Tier Security Levels" has provided a means of storing patients' health records in the cloud by ensuring that these records are secure by the use of the above listed security mechanisms which ensures that only authorised persons have access to the patients' health records.

References

- Abayomi-Alli, A.A., Ikuomola, A.J., Robert, I.S and Abayomi-Alli, O.O. (2014). An Enterprise Cloud-Based Electronic Health Records System. *Journal of Computer Science and Information Technology*,2 (2), 21-36.
- Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). Cloud computing: Security model comprising governance, risk management and compliance. In 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC) (pp. 1–6). <http://doi.org/10.1109/ICDMIC.2014.6954232>
- Chelladurai, U. and Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing* 13 (1), 693-703.
- Kluge, E. W. (2020). *The Electronic Health Record: Ethical Considerations*. London. Academic Press Elsevier.
- Li, M., Yu, S, Zheng, Y. and Ren, K.(2012). Scalable and secure sharing of personal health records in cloud computing using Attribute-based Encryption. *IEEE Trans Parallel Distributed System*;1–14.
- Nagy, A. (2005). *The Impact of E-Learning. E-Content: Technologies and Perspectives for the European Market*. Berlin: Springer-Verlag, 79–96.
- Sharma, M. K. (2011). e-governance applications in public healthcare for rural areas of uttarakland," *Computer*



society of India communication, India, vol. 35, issue 7, pp. 8-10

Sharma, Y. & Balamurugan, B.(2020). Preserving the Privacy of Electronic Health Records using Blockchain. *Procedia Computer Science*(173). Retrieved from <https://doi.org/10.1016/j.procs.2020.06.021>.

Srivastava, S., Pant, M., Abraham, A and Agrawa, N. (2015). The Technological Growth in e-Health Services. *National Institutes of Health*. doi: 10.1155/2015/894171

Yang, G., Li, C. and Marstein, K.E. (2021). A blockchain-based architecture for securing electronic health record systems. *Concurrency and Computation: Practice and Experience* 33 (14), e5479.

Teng, C., Mitchell, J. and Walker, C. (2010). A Medical Image Archive Solution in the Cloud. In *Proceedings of the 2010 IEEE International Conference on Software Engineering and Service Sciences (ICSESS)*, Beijing, China, pp. 431–434.

Walters, P. (2021). What is eHealth? <https://www.truevault.com/ehealth>

Yaw, S.A.A., Twum, F., Hayfron-Acquah, J. B. and Panford J. K.(2015). Cloud Computing Framework for E-Health in Ghana: Adoption Issues and Strategies: Case Study Of Ghana Health Service, https://www.researchgate.net/publication/277930258_Cloud_Computing_Framework_for_EHealth_in_Ghana_a_Adoption_Issues_and_Strategies_Case_Study_of_Ghana_Health_Service

