A SECURE G-CLOUD-BASED FRAMEWORK FOR GOVERNMENT HEALTHCARE SERVICES

[1]Boosa Ramya, [2]DR.N. chandramouli
[1]mtech, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, H. No:20S41D5803, ramyaboosa88@gmail.com,
[2]Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, CMNASINGOJU@gmail.com

ABSTRACT: Within the literature, we have witnessed in the healthcare sector, the growing demand for and adoption of software development in the cloud environment to cope with and fulfill current and future demands in healthcare services. In this paper, we propose a flexible, secure, cost-effective, and privacy-preserved cloud-based framework for the healthcare environment. We propose a secure and efficient framework for the government EHR system, in which fine-grained access control can be afforded based on multi-authority ciphertext-policy attribute-based encryption (CP-ABE), together with a hierarchical structure, to enforce access control policies. The proposed framework will allow decision-makers in Saudi Arabia to develop the healthcare sector and to benefit from the existing e-government cloud computing platform ‘‘Yasser,’’ which is responsible for delivering shared services through a highly efficient, reliable, and safe environment. This framework aims to provide health services and facilities from the government to citizens (G2C). Furthermore, multifactor applicant authentication has been identified and proofed in cooperation with two trusted authorities. The security analysis and comparisons with the related frameworks have been conducted.

Keywords *– Cloud computing, electronic health record, security, attribute-based encryption, ciphertext policy, identity proofing, authentication, authorization.*

1. INTRODUCTION

A common phenomenon in healthcare in most Arab countries is the lack of optimal utilization of human and material resources available to provide integrated healthcare to prevent diseases and treat diseases after they occur. Statistics indicate that Arab countries suffer from high rates of health problems, such as diabetes, liver disease, and parasitic diseases, such as histosomiasis and malaria. These health problems could be prevented before they occur or their complications prevented by early detection. This is due to a combination of factors: planning, operational, and technical. If we were able to overcome them, this would lead to significant progress in the level of health care. In addition, there is a weakness and lack of available hospital information systems, which is some of the most advanced software that directly serves all technical and administrative healthcare activities, ensuring that the medical institution has full control over all its activities and resources. The successes of these advanced systems do not depend on he exact selection of equipment and software for storage. Rather, their success depends on their suitability for different users—from healthcare providers, such as doctors, nurses, technicians, and even administrators—where the vision and priorities of each of these categories differ, and their information needs vary, as do the benefits of each of these systems. The traditional health system (paper) has been replaced by an electronic health information system because the traditional system has been found to be ineffective due to a number of issues, including low storage capacity, high operating and maintenance costs, and system integration [1]. The computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features [2]. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare [2], [3].

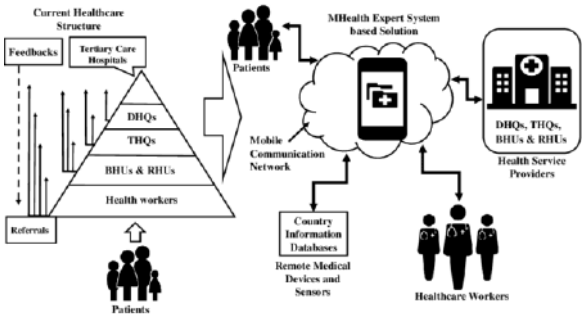

Fig.1: Example figure

The rapid shift to the cloud and its use in healthcare systems has raised concerns about crucial issues of privacy and information security [4], [5]. The adoption of the cloud in IT increases the focus and concern of healthcare providers on clinical and patient-related services and reduces attention on infrastructure management [6]. The sharing of personal and health information across the Internet and various servers outside the safe environment of the healthcare institution has led to a number of problems related to privacy, security, access, and compliance issues [7]–[10a].

2. LITERATURE REVIEW

A review of cloud computing technology solution for healthcare system:

Previously the traditional healthcare information system that used in the healthcare sector was the paper-based and then later it was replaced by the Healthcare Information System (HIS). However the HIS was found not perform effectively because of several issues such as storage capacity, system integration, high operating cost and system maintenance. Cloud computing is a new technology that deliver the software, infrastructure and computational platform as a service over the Internet in any place and any time. This technology has been said can solve many problems of the healthcare system such as increase the storage capacity and add new capability on the existing healthcare system. Cloud computing offers cost effective, increase interoperability and accessibility, optimize resources and integrate the healthcare information systems. It becomes a solution for solving the current issues, which lead to enhance functionality and features of the healthcare information systems. Therefore, the aim of this study is to explore the cloud computing technology as solution for healthcare information system issues. Issues such as data transmission, data storage, cost and maintenance issues are presented and described. The implications of this study then discussed.

A descriptive literature review and classification of cloud computing research

We present a descriptive literature review and classification scheme for cloud computing research. This includes 205 refereed journal articles published since the inception of cloud computing research. The articles are classified based on a scheme that consists of four main categories: technological issues, business issues, domains and applications, and conceptualising cloud computing. The results show that although current research is still skewed towards technological issues, new research themes regarding social and organisational implications are emerging. This review provides a reference source and classification scheme for IS researchers interested in cloud computing, and to indicate under-researched areas as well as future directions.

Addressing cloud computing security issues

The recent emergence of cloud computing has drastically altered everyone’s perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon

cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

Impact of cloud computing on health care

The term "Cloud Computing" is a recent buzzword in the IT world and has been a major topic of conversation as of late and is emerging as one of the most important technologies of this decade. Large technology companies are already investing millions of dollars in building infrastructure, services and applications to make cloud computing easily accessible to consumers, organizations and businesses. It remains to be seen how cloud computing will impact the healthcare business since it is very diverse and complex, it presents several challenges such as protecting members health records in addition to following HIPAA guidelines set by federal compliance regulations Efforts are being made to decrease the costs for consumers and it will play a big role in achieving it and also improving clinical and quality outcomes for patients. It will be very interesting to see how cloud computing will address and contribute towards these issues in the healthcare industry. Cloud computing field has an immense potential in it to be used in the field of healthcare especially developing countries like India. This article will discuss briefly on the inception of cloud computing and what it exactly is.

Securitychallenges in healthcare cloud computing: A systematic review

Healthcare data are very sensitive records that should not be made available to unauthorized people in order for protecting patient's information security. However, in progressed technologies as cloud computing which are vulnerable to cyber gaps that pose an adverse impact on the security and privacy of patients' electronic health records and in these situations, security challenges of the wireless networks need to be carefully understood and considered. Recently, security concerns in cloud computing environment are a matter of challenge with rising importance. In this study a systematic review to investigate the security challenges in cloud computing was carried out. We focused mainly on healthcare cloud computing security with an organized review of 210 full text articles published between 2000 and 2015. A systematic literature review was conducted including PubMed, Science direct, Embase, ProQuest, Web of science, Cochrane, Emerald, and Scopus databases. Using the strategies described, 666 references retrieved (for research question one 365, research question two 201, and research question three 100 references). Review of articles showed that for ensuring healthcare data security, it is important to provide authentication, authorization and access control within cloud's virtualized network. Issues such as identity management and access control, Internet-based access, authentication and authorization and cybercriminals are major concerns in healthcare cloud computing. To manage these issues many involved events such as Hybrid Execution Model, VCC-SSF, sHype Hypervisor Security Architecture, Identity Management, and Resource Isolation approaches have to be defined for using cloud computing threat management processes.

3. METHODOLOGY

- Li *et al.* enhanced a Multi-authority Attribute base encryption (MA-ABE) scheme to handle efficient and on-demand user revocation, and prove its security. The proposed MA-ABE scheme utilized ABE to encrypt and access not only the patient data but also various users from public domain with different professional roles, qualifications and affiliations.
- Alshehri *et al.* proposed a cloud-based EHR system, which consists of the cloud-based data storage and computing resources, healthcare providers, and attribute authority (AA). In this scheme, one single AA is responsible for key management, including generation, distribution, and revocation in the EHR system.

Disadvantages:

- In the literature, there are no existing powerful frameworks that clearly address all viable schemes and interrelationships between cloud computing and healthcare technology.
- The problem with the ABE-based encryption scheme is that data encryption needs to use the public key for each licensed user and needs to use attributes to control the user's access to the system. So,

ABE cryptographic credentials are issued by trusted attribute authority, which is in possession of a global master key for key generation.

In the proposed system, it provides a flexible, secure, cost-effective, and privacy preserved G-cloud-based framework for government healthcare services. The proposed system is developed by applying, using, and modifying the most recent encryption and decryption mechanisms suited for cloud-based EHR systems.

- The proposed scheme does not use the standard encryption system, which is not suited to the cloud environment. Achieving scalability of computing resources that can be expanded and controlled according to the required health services. The EHR is able to support massive data exchanges.
- The proposed system is developed by providing an effective solution for decision makers in the government health sector to adopt cloud-based healthcare systems, especially in developing countries.
- Different domains of attributes are managed by different attribute authorities, which operate independently from each other and controlled by the central trusted authority.

Advantages:

- Providing a better authentication multifactor applicant authentication in cooperation with two trusted authorities.
- Security analysis has been conducted according to major security requirements in cloud environments.
- This framework aims to provide health services and facilities from the government to citizens (G2C).
- Our proposed framework is based on CP-ABE which is more secure and more efficient in comparison with other existing frameworks. It uses multiple authority attribute domains that impose different access privileges for different types of applicants in order to achieve fine-grained access control.
- The proposed scheme is suited for G-based cloud EHR systems and gets advantages from the facilities and the infrastructure provided by the government.

A cloud-based theoretical framework has been developed for the improvement of electronic health services in Saudi Arabia. The proposed framework will allow decision makers to develop the health sector and to benefit from the services provided by other sectors in the kingdom, such as the electronic services system called ‘‘Absher,’’ which is used by the Ministry of the Interior to ensure the personal identity of the beneficiaries, and the e-government cloud computing platform ‘‘Yasser,’’ which is responsible for delivering shared services through a highly efficient, reliable, and safe environment. The proposed framework uses cloud computing to develop health services provided by the Ministry of Health to citizens. This framework aims to provide health services and facilities from the government to citizens (G2C) in the kingdom.

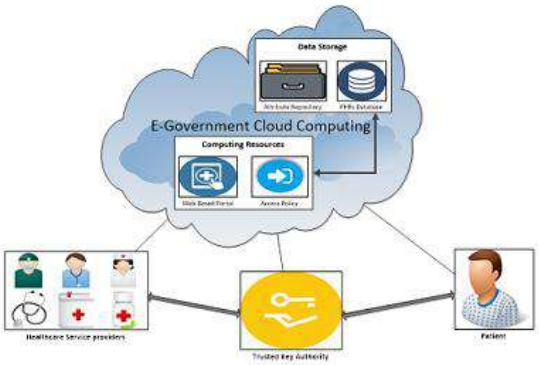

Fig.2: System architecture

Figure shows the proposed cloud-based framework, which consists of four fundamental entities. These entities interact with one another directly and indirectly to perform their tasks in the cloud-based EHR framework.

4. IMPLEMENTATION

MODULES:

- Patient
- HCP
- E- Cloud System
- Trusted Authority

MODULES DESCSRIPTION:

PATIENT

In this module, there are n numbers of Patient are present. Patients should register before doing some operations. And register Patients details are stored in Patients module. After registration successful he has to login by using authorized HCP name and password.

Patient, based on the characteristics of HCPs to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server.

In this module, we do the following functions:

1. Register
2. Login
3. Upload File
4. View File
5. Logout

Patients should specify the access policy for each data attribute in the EHR, so that the data HCP can only access and decrypt his authorized data attribute.

HCP:

The HCP is the cipher texts receiver who can access the outsourced data. The HCP is able to decrypt the initial and re-encrypted cipher texts if he is the intended receiver defined by the Patients or data disseminators. In this module, there are n numbers of data HCPs are present. Data HCP should register before doing some operations. And register HCP details are given permission from the trusted authority only. After registration successful the trusted authority has to give permission for the data HCP. Only after that the HCP has to login by using authorized HCP name and password. In this module, the HCP can specify their roles like Surgeon, Insurance etc.

E-Cloud System

In this module, we develop the following functionalities:

1. Login
2. View All File Information
4. Update HCP and Patients
5. View All Patient

Trusted Authority:

The central authority (CA) is a fully trusted authority running on trusted cloud platform with flexibility and scalability that manages and distributes public/secret keys in the system, including generates system parameters to initialize system and generates private keys and attribute keys with HCPs' identity and attributes.

5. EXPERIMENTAL RESULTS

Fig.3: Home screen

Fig.4: Patient registration

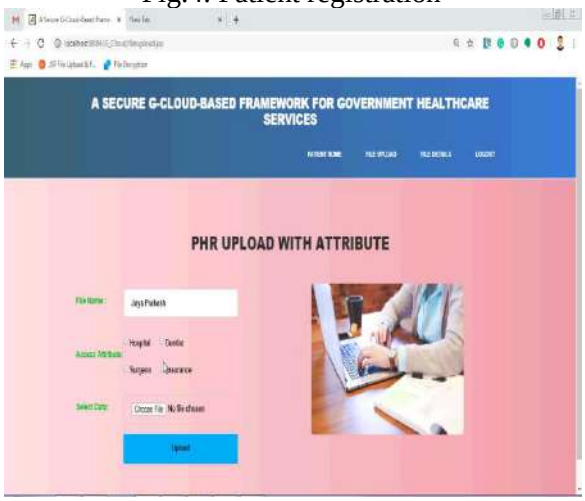

Fig.5: PHR upload

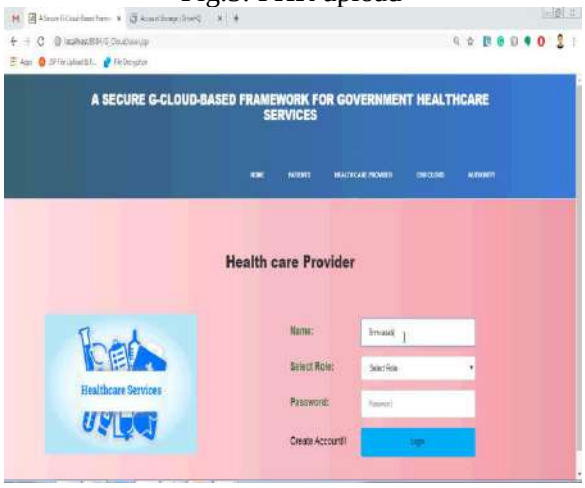

Fig.6: healthcare provider

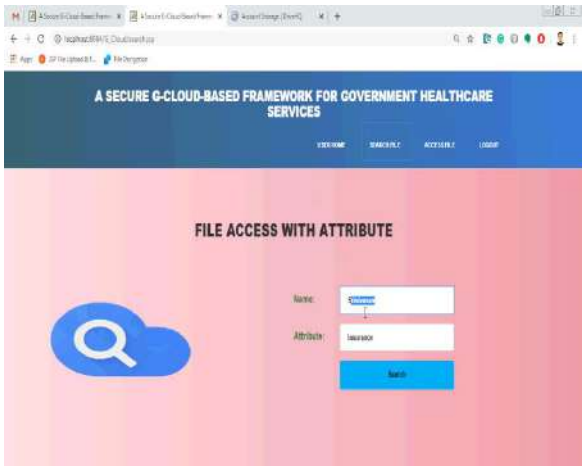

Fig.7: File access with attribute

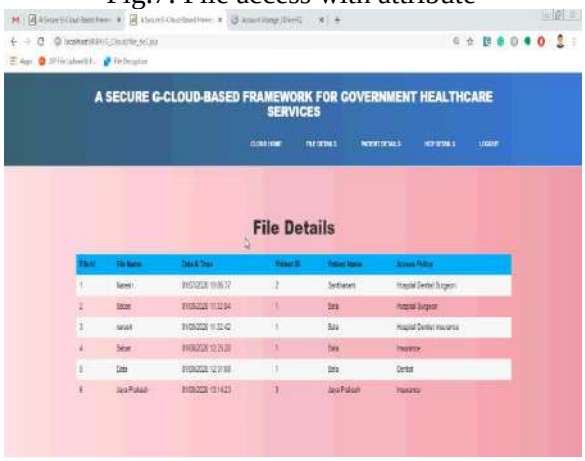

Fig.8: File details

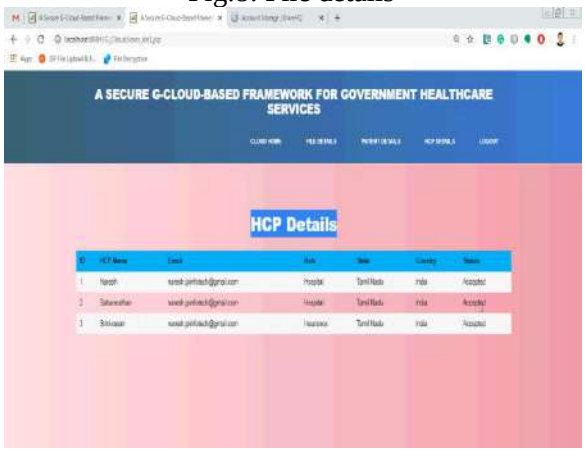

Fig.9: HCP details

6. CONCLUSION

In this paper, we proposed a secure cloud-based EHR framework that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers,patients, and practitioners. In the framework, the attribute domain authority manages a different attribute domain and operates independently. In addition, no computational overhead is completed by the government authority, and multifactor applicant authentication have been identified and proofed. The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treatment services to the majority of citizen patients.

Future work includes implementing and evaluating the proposed scheme in a real-world environment.

REFERENCES

[1] M. Masrom and A. Rahimli, ``A review of cloud computing technologysolution for healthcare system," *Res. J. Appl. Sci., Eng. Technol.*, vol. 8,no. 20, pp. 2150_2155, 2014.
[2] A. Hucíková and A. Babic, ``Cloud Computing in Healthcare: A Space ofOpportunities and Challenges," *Transforming Healthcare Internet Things*,vol. 221, p. 122, 2016.
[3] H. Yang and M. Tate, ``A descriptive literature review and classification ofcloud computing research," *CAIS*, vol. 31, Apr. 2012, Art. no. 2.
[4] D. Zissis and D. Lekkas, ``Addressing cloud computing security issues,"*Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583_592, 2012.
[5] V. K. Nigam and S. Bhatia, ``Impact of cloud computing on health care,"*Int. Res. J. Eng. Technol.*, vol. 3, no. 5, pp. 1_7, 2016.
[6] *How to Improve Healthcare with Cloud Computing*, Hitachi Data Systems,Santa Clara, CA, USA, 2012.
[7] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, ``Securitychallenges in healthcare cloud computing: A systematic review," *GlobalJ. Health Sci.*, vol. 9, no. 3, p. 157, 2016.
[8] D. Sun, G. Chang, L. Sun, and X. Wang, ``Surveying and analyzing security,privacy and trust issues in cloud computing environments," *ProcediaEng.*, vol. 15, pp. 2852_2856, Jan. 2011.
[9] N. Khan and A. Al-Yasiri, ``Identifying cloud security threats to strengthencloud computing adoption framework," *Procedia Comput. Sci.*, vol. 94,pp. 485_490, Jan. 2016.
[10] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, ``Securityissues for cloud computing," *Optimizing Inf.Security Advancing PrivacyAssurance: New Technologies: New technol.*, vol. 150, 2012).

