iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** II **Month of publication:** February 2020

DOI: http://doi.org/10.22214/ijraset.2020.2054

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

Implementation of Authorization Framework for EHR Services using Enhanced Attribute Based Encryption

K. Rajathi[1], Mrs. S. Sivasankari[2]
[1]*Research Scholar, Department of Computer Science & Application, PRIST University, Madurai Campus.*
[2]*MSc., M.Phil., Assistant Professor, Department of Computer Science & Application, PRIST University, Madurai Campus.*

Abstract: ***Electronic Health Record (EHR), which is based on cloud systems are with the features like big storage, clinical research with efficiencies as well as fostering collaborative care with several improvements for the future generation. In the past years we experienced the great development in the data-storage of cloud system's Electronic Health Records (EHRs), here in this the integration of electronic systems and cloud computing is developed to make the medical information exchanges easy between patients as well as the healthcare centers; it generates these kind of centers to do their work in low economic way along EHRs availability. So it is needed to improve an authoritative form to proceed well guarded EHR Service management. Thus the novel is given in a scrutinized form, which make use Attribute Based Encryption (ABE) with high safety for the information of patients. So this kind of framework, which is there in the edge will developed with the usage of Enhanced Attribute Based Encryption (E-ABE); for providing safe transformation of information by sharing data for organizations. This research work contains a novelistic approach with the ideology of prototype which is developed for the evaluation of framework. So this system gives the data of patients to medicine dealers on the basis of EHR system.***

Keywords: Attribute Based Encryption, Attribute Based Access Control, Electronic Health Record, Cloud Storage, Semantic Web, Access Broker, Knowledge Graph, Cloud Computing

I. INTRODUCTION

Electronic health record (EHR) systems provides several secured research on clinical basis and healthcare services. EHRs contains related healthcare information in several aspects like genomic test results, diagnoses, medication, laboratory test results, and imaging data. IBM, a vast data with three important properties like volume, variety, and velocity.1. It is evidential that it contains an important "big EHR data" with the issues of management like volume, veracity, and velocity. EHR-based systems with inadequate data will put the life of patient in risk. 2. The main security deals with the security of storage, access and retrieval. 3. Besides the control mechanism, the location of accessing the information is mandatory for the security of data. Recent data corruption of patients are the real stipulation for dual researches on the security of information with location.

These services use abundantly mobile devices for efficient services. Attributed-based encryption (ABE) was introduced by Sahai and Waters, here the patients can give data as per their wants [1]. Goyal etal. gives clarification of ABE [2],it

controls the encryption of information through private settings and policies. It contains ciphertext-policy ABE(CP-ABE) and key-policy ABE (KP-ABE)as per the various policies of attributes. KP-ABE is a scheme where every private key is connected to the access structure. In cipher text policy of ABE, dealers can express the policy, by considering the decryption message of receivers in the algorithms of encryptions. Bethencourt et al.was presented by the former mentioned[3]. The system permits the encryptor to make use of patients information. Author felt that the generic group model was a secured thing and proved it too, with the use of oracle they can proceed a group operation. Goyal et al. introduced generic infrastructure to shift a key-policy ABEscheme into a ciphertext-policy ABE scheme [4],its form and size will be number 3, here*n* is the number of attributes spent in thedecryption policy. This CP-ABE schemes is vital, based on ciphertext size will be there in [5], and its size depends linearly on attributes number gets involved in this specific case for ciphertext. In schemes like CP-ABE the ciphertexts size get differs and it is based total variant of attributes indulged in ciphertext policies. Emuraet al. introduces a stable size for CP-ABE scheme[6], yet it is very protective it lacks random oracles, it denotes the encryptor faces several challenges before they prepares a phase. And so it is considered as a volatile one; by comparing with protective security. Till CP-ABE scheme contains rigid ciphertext size with high safety with lack of random oracles. So the use numerous electronic devices raises the need of security and pave way for several private settings. So the mandatory thing, which is relevant to our research process is to save and manage with security accessibility of big EHR information. Then the usable services of this system, storage comes with extra features in combination with technologies of mobile like updated form of EHR regarding its cost and management along with collection of information. Several vast EHR cloud data can be stored in Electrocardiography (ECG) with private securities besides an authoritative outlet is given to EHR with Enhanced Attribute Based Encryption method for multiple users.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

II. RELATED WORK

Hur, Junbeom, introduced efficient and secured information sharing technique and this they offer CP-ABE novelistic scheme for this with the upcoming accomplishments. This research work issues related to Escrow and proxy encryption are cleared with this ABE technique. Yu, Shucheng *et al.*[3] proposed data sharing on the basis of attribute as well as attribute revocation; along it gives appropriate remedy on the basis of novel cryptographic methods. The contents will be given by semi-trustable proxy servers and it is done on the basis of servers of that kind itself among numerous users and the authenticated security will be given with the several policies in the network 3.

Fuzzy Identity Based Encryption was proposed by A. Sahai and B. Waters with two constructions. And those two constructions are with the resemblance of IBE with the identification of Fuzzy. The above mentioned IBE are resistant to error and withstand the attack of collusion and random oracles are not used in this constructions as well as they make use of Selective ID security model for the privacy and security of data, which will repellent to error and withstand attacks of collusion. ABE, attribute based encryption data will be introduced for control of access, here secret code of user and cipher texts are related attribute sets. At the time of collision of cipher text and secret key, user can decrypt that text.

ABE is considered as a root for CP-ABE, it focuses to create a secured form of ABE cryptosystem. This system contains labeled encryptor with expressive attributes. Every private key is linked with access construction with the specification of ciphertext decryption of the key. And this kind of procedure is named as Key-Policy Attribute-Based Encryption (KP-ABE), as it works by depending on the private key; here the ciphertexts are with the identification of descriptive attributes. And here the users can decrypt a ciphertext whether it correlates with the key's access structure. And this framework supports features of which subsumes Hierarchical Identity-Based Encryption (HIBE) [5].

Bethencourt *et al.*[6]proposed Ciphertext-Policy Attribute Based Encryption and they gives the former construction of a ciphertext-policy attribute-based encryption (CP-ABE) for this issue. This system connects the private key of user with an arbitrary number of attributes those are presented as strings. At the time of third person's encryption of messages in this system it will be identified through access structure over attributes. Users can decrypt a ciphertext if their access pass through its structure. From mathematical perspective, these access structure are noted as monotonic "access tree", these access structures are made of threshold gates and attributes are left behind. And the system is created for Ciphertext-Policy Attribute Based Encryption. And this system permits us to encrypt the private key of users are identified with attributes meanwhile the person who encrypt the information can get the policy through specification of attributes, where we can decrypt. And it allows schemes to proceed in a structure of monotonic along with the repellence to attacks of collision; where a person who attack may obtain several private keys. At the end, it comes with the development in this system along numerous techniques of optimization6.

R. Ostrovsky *et al.* [7]introduced Attribute-Based Encryption with Non-Monotonic Access Structures. It gives anew Attribute-Based Encryption scheme; in which a private key can provide any formula of assessment for non-monotone ones over its attributes.

Alfin Abraham *et al.*[9] introduced valid revocation IBE survey at the same time a they found remedy to mitigate the borders of IBE in connection to revocation in regard to past remedies. In the case of having large number of users, they decides to keep away interaction from the key update in the case of vast numerical users by having the PKG online at cut-throat9.

Di Vimercati *et al.*[10] introduced Over-encryption: it deals with the maintenance and utility of outsourced information. Here they found a remedy to come out they issues, by updating outsourcing information in further features, and it includes vast resources with notable size, re-encryption and re-transmission of the user might not accepted to some extend.

Ibraimi *et al.*[11]proposed Mediated cipher text policy attribute-based encryption with its application and the very new scheme is proposed for revocation of attribute in CP-ABE called mediated Cipher text-Policy Attribute-Based Encryption (CP-ABE). Here they divided the secret key into two for the mediator and for the users.

III. PROPOSED APPROACH

Development of secured, ABE mechanism for cloud based HER services with flexibility in accessing and encrypting a data is considered as the main objective. With the usage of technologies like OWL, ABE technique and SWRL we can construct a new EHR technique with the possibility to share an information in an easily secured manner. An outlet of EHR system is seen there inFigure 1; and it is categorized into four levels. In level 1, users are asked to access their interested EHR. In level 2, the authentication process takes place; starting from attributes of users and EHR by accessing its terms and policies. And these attributions are encrypted with the concern of EHR. And level 4 plays the role of Cloud servicer for sending and receiving data. Here levels of odd number comes under the category of inner organizational edge while the level for stands for outside of it; which is meant for lack of trust.

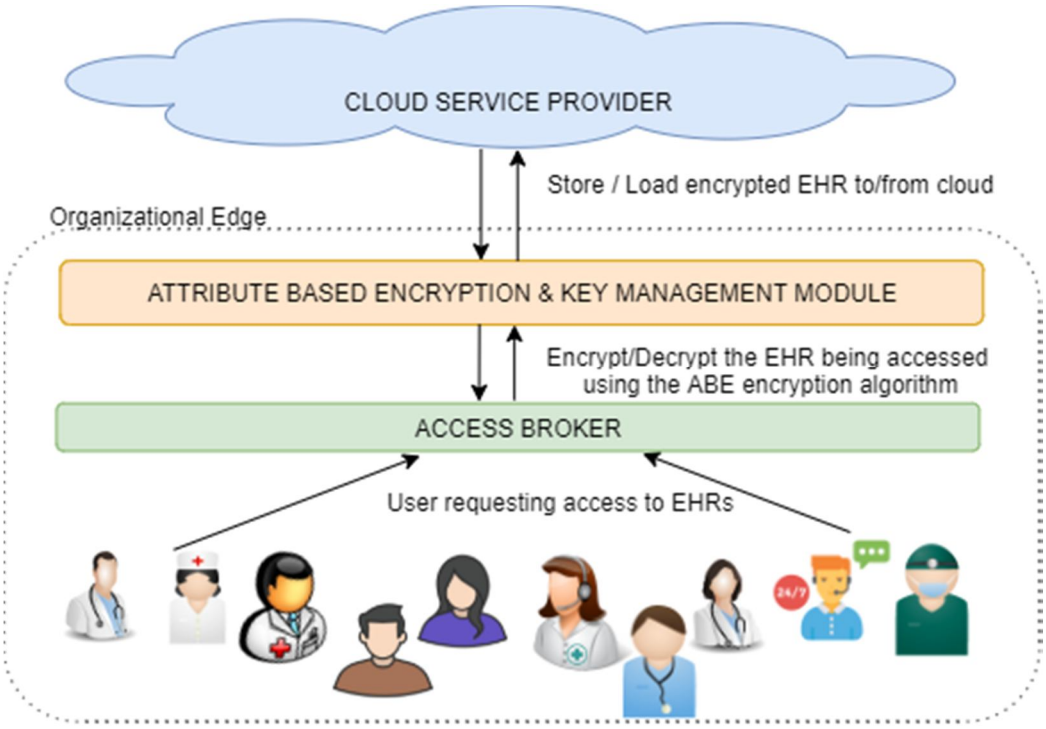


Figure 1: Our System is composed of four levels

IV. SYSTEM ARCHITECTURE

Here the construction system with its four major models is given in the figure 2; and they are Access Broker, Encryption Unit, Key Generation Unit and EHR Ontology. And the information will be provided in the following way, medical dealers are the one accessing the system with their credentials and this process undergoes the process of authentication through the Access Broker. The former module [16] used Attribute Based Access Control is there to proceed with control on access mechanism to deal the policy rigidly and to take firm decision. As mentioned in the 5th section, we should proceed to next division to access permission like modification of data by rewriting. Then it proceeds with the accessing of EHR by the users. And the updation of data will be done by Encryption Unit.

This unit uses ABE for encrypting the EHR field.

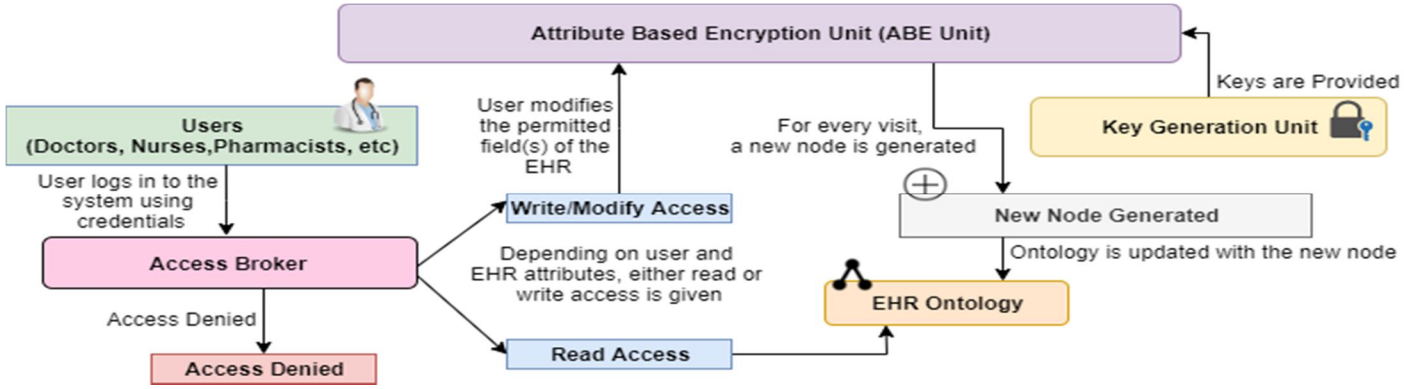


Figure 2: System Architecture

EHR ontology is questioned by Attribute Extraction Unit for retrieving field attributes of users and EHR. As those information are stored as node format in a graph, querying is considered as a simple task. And those process are done through SWRL rules.

The Organizational Knowledge Base, contains the storage of all attributes stakeholders of the institution of HIPAA compliant EHR Ontology. It consists of the attributes and activities of various stakeholders of several medical organization and the bond lies between them.

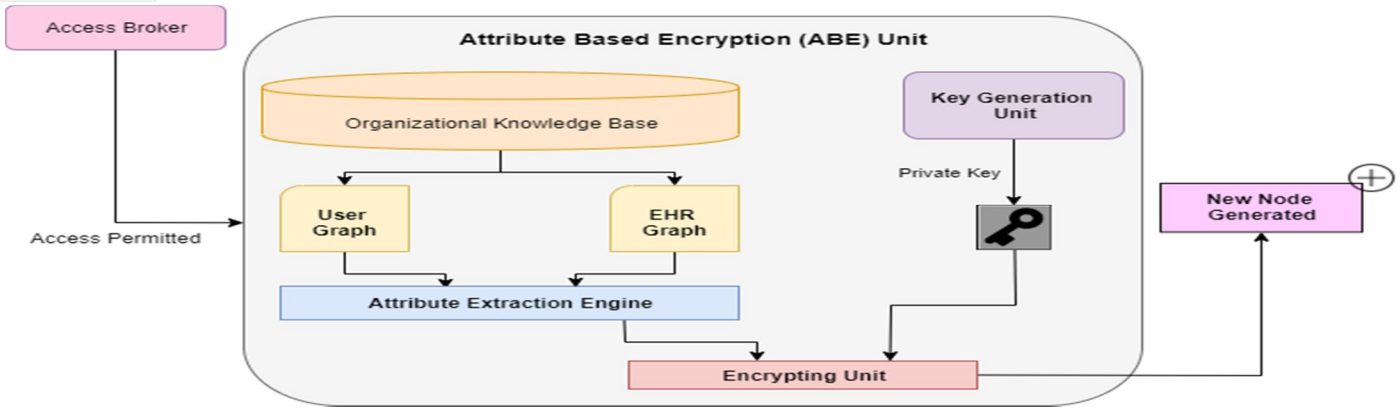


Figure 3: Encryption Unit Architecture

The keys needed for the process of encryption/decryption will be provided by the Key Generation Unit, which is described in the former section and for this process it ought to access the Organizational Knowledge Base shown as Figure 3. And this is created with the unification of users and EHR field attributes of ABE unit to deal with encryption. And the same thing is followed for the process of decryption; then it decrypts the exact EHR field to the user.

The Encrypting Unit is just like a representator for various sub-modules under ABE Unit as it having access with the Key Generation Unit, the Organizational Knowledge Base and the Attribute Extraction Unit. It needs the guidelines of KGU for collecting the secret keys for the process of both encrypt/decrypt. In order to proceed this encryption, both attributes and its value is needed and it is there in Attribute Extraction Unit.

V. SYSTEM IMPLEMENTATION

Key Generation Unit, contains encryption keys and those text which are encrypted ought to be generated in EHR Ontology. For this purpose, they creates a node and collects the details of patient's visit of that organization. The encrypted text then needs to be updated in the EHR Ontology. To do this, a new node is created which records all the details of a patient's visit to the medical organization. At last this ontology gets stored in the provider of cloud service. And mathematical representation of implemented system is given before.

User set G = {G1, G2, ...Gn}
User Attribute Set GX= {GX1, GX2, GX3, ...GXn}
EHR set P = {P1, P2, ...Pn}
EHR attribute set PS = {PX1, PX2, PX3, ...PXn}
EHR Fields Set UV = {UV1, UV2, ...UVn}
EHR Fields Subset UVS ⊂ UV
Policy set RX = {RX1, RX2, ...RXn}
Decryption Policy set MS = {MS1, MS2, ...MSn}
∀ User G, ∃ User Attribute Set GS
For evaluating access decision
For each User G ∧ EHR T∧ EHR Data Set M,
If GXsatisfies any one from policy from RX→
Read and or Write (User G , EHR T, GX)
For data encryption using ABE in EHR
For each User G ∧ EHR T, ∃ Fields Subset UV,
V ∧ A ∧ Data User Attribute Set GX ∧ M → EHR Encrypted data
where KX ⊂ MX
For data decryption using ABE in EHR
If Data Attribute Set KX ⊂ MX
KX ∧ TY → EHR Decrypted data

Sub-modules will be explained as follows.

1) *EHR Ontology:* The *EHR Ontology* is an ontology of HIPAA complaint [10] ithas theattributes of users and EHR as noted in graph. It contains the roles and attributes of numerous stakeholders of their organisation and a bond between them.
2) *Cloud Service Provider:* It is a common platform. And the data hosting the EHR Ontology gets shifted to provider of cloud service.

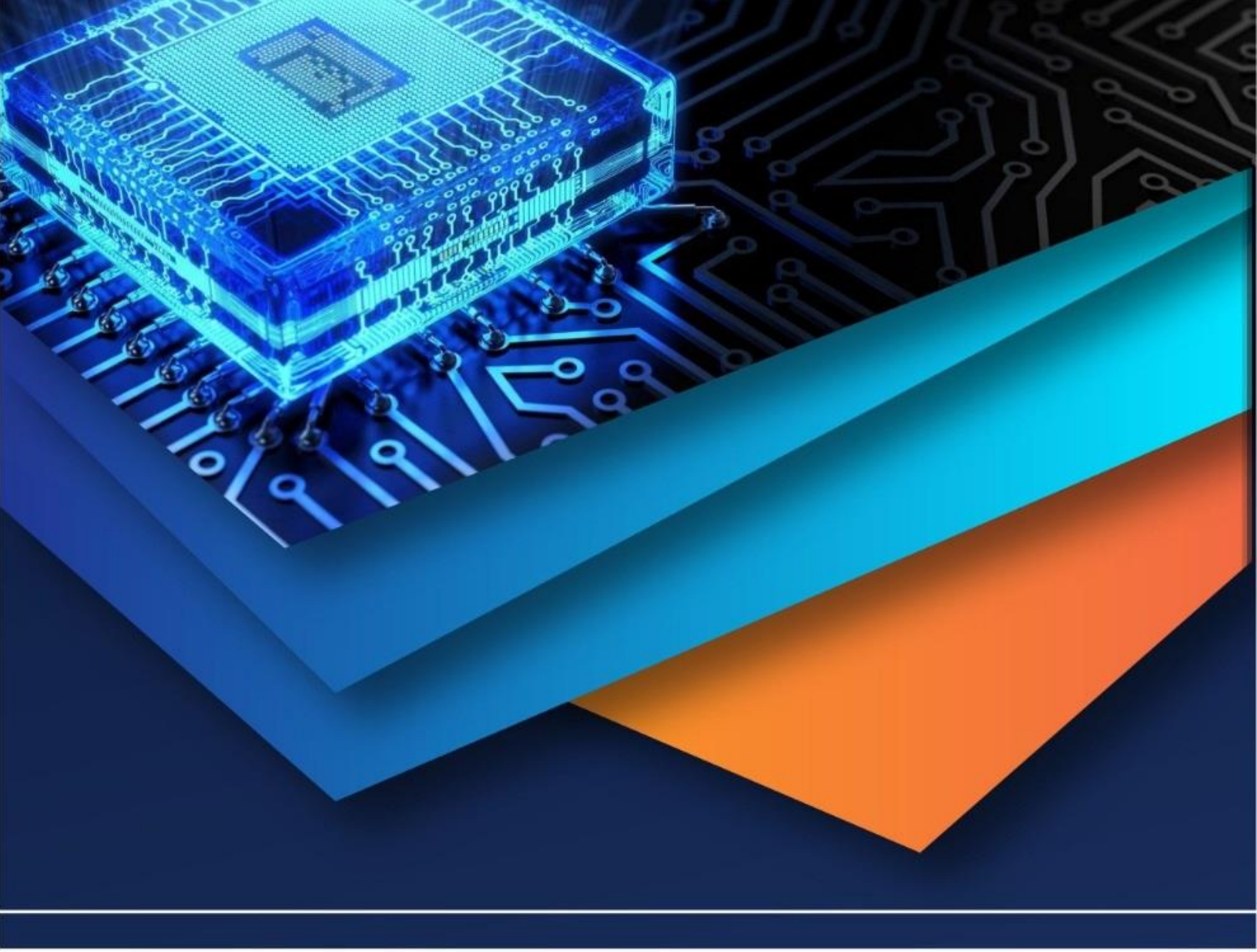
VI. CONCLUSION

Service of EHR os there to maintain the data of patients with ensured securities to adhere by regulatories. Meanwhile it is must to access the medical information patients to caretakers to help the patients in need. The security ofthis system is doubt's as it is frequently accessed by the end users. And a novel has been created and it depends onattribute based authorization mechanism for EHR services, so it encrypt the data of patients securely by coping with the policies of medical organisation. And it transfers the service management from patient to organisation for easy cloud delegation.

In our further research work, data exchange of EHR and the vital functions of inter organisational EHR system gets included. Further privacy issues fevar song tha safety office data will be researched in future. For example, rigid mechanism of authentication will prevent strangers from accessing a credentials doctors then machine learning ML is used to find the ananmalous pattern involved.

REFERENCES

[1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E.Youman, “Role-Based Access Control Models,” Computer, vol. 29, no. 2, pp. 38–47 (1996).
[2] Hur, Junbeom “Improving security and efficiency in attribute-based data sharing”, IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October (2013).
[3] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou.,”Attribute based data sharing with attribute revocation”, In Proceedings of the 5th ACM Symposium on Information Computer and Communications Security, pp. 261-270. ACM, (2010).
[4] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption”, Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt ’05), pp. 457-473 (2005).
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data”, Proceedings of ACM Conference on Computer and Communication Security, pp. 89-98 (2006).
[6] J. Bethencourt, A. Sahai, and B. Waters, “CiphertextPolicyAttribute Based Encryption”, Proceedings IEEE Symposium Security and Privacy, pp. 321-334,(2007).
[7] R. Ostrovsky, A. Sahai, and B. Waters, “AttributeBased Encryptionwith Non-Monotonic AccessStructures”,Proceedings ACM Conference Computer and Comm. Security, pp. 195-203 (2007).
[8] K. Hayrinen, K. Saranto, and P. Nyk ¨ anen, “Definition, structure, ¨ content, use and impacts of electronic health records: a review of the research literature,” International journal of medical informatics, vol. 77, no. 5, pp. 291–304, 2008.
[9] “Electronic health record-system functional model, release 1,” in ANSI/HL7 EHR, R1-2007. ANSI/HL7, 2007.
[10] R. C. Barrows Jr and P. D. Clayton, “Privacy, confidentiality, and electronic medical records,” Journal of the American Medical Informatics Association, vol. 3, no. 2, pp. 139–148, 1996.
[11] D. Blumenthal, “Launching hitech,” N Engl J Med, vol. 2010, no.362, pp. 382–385, 2010.
[12] C. for Disease Control, Prevention et al., “Hipaa privacy rule and public health. guidance from cdc and the us departmentof health and human services,” MMWR: Morbidity and mortality weekly report, vol. 52, no. Suppl. 1, pp. 1–17, 2003.
[13] U. D. of Health, H. Services et al., “Summary of the hipaa privacy rule,” Washington, DC: Author. Retrieved December, vol. 2, p. 2007, 2003.
[14] A. Bahga and V. K. Madisetti, “A cloud-based approach for interoperable electronic health records (ehrs),” IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 5, pp. 894–906, 2013.
[15] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE transactions on parallel and distributed systems, vol. 24, no. 1, pp. 131–143, 2013.
[16] S. Chandra, V. Karande, Z. Lin, L. Khan, M. Kantarcioglu, and B. Thuraisingham, “Securing data analytics on sgx with randomization,” in European Symposium on Research in Computer Security (ESORICS), 2017, pp. 352–369.
[17] F. Schuster et al., “Vc3: Trustworthy data analytics in the cloud using sgx,” in IEEE Symposium on Security and Privacy. IEEE, 2015, pp. 38–54.
[18] J. A. Evans, “Electronic medical records system,” Jul. 13 1999, uS Patent 5,924,074.
[19] E. H. Shortliffe et al., “The evolution of electronic medical records,” ACADEMIC MEDICINE-PHILADELPHIA-, vol. 74, pp. 414–419, 1999.
[20] M. Lavin and M. Nathan, “System and method for managing patient medical records,” Jun. 30 1998, uS Patent 5,772,585.
[21] S. Narayan, M. Gagne, and R. Safavi-Naini, “Privacy preserving ´ ehr system using attribute-based infrastructure,” in CCSW, 2010.
[22] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY