Implementing a Cloud-Based Security Framework to Automate Healthcare Operations

Arpita Bhatia[1], Neha Yadav [2], Pankaj Pateriya [3]
[1] *IPS Academy, Institute of Engineering & Science, Indore*
[2] *IPS Academy, Institute of Engineering & Science, Indore*
[3] *IPS Academy, Institute of Engineering & Science, Indore*
(E-mail: arpitabhatia31@gmail.com, nehalav1621@gmail.com, ppateriya@gmail.com)

ABSTRACT - Security and privacy will always be future challenges looming for researchers and authors. These challenges encompass authentication, authorization, integrity, confidentiality, availability, and privacy. These are major concerns, owing to third party communications that lead to possible loss of data from one side to another. Multi-dimensional confidential data are stored in EHR maintenance, that is, the patient's personal and medical history. Medical history includes items such as laboratory results and demographic data; billing data for medical services; test reports from pathologists, radiologists, or other diagnostic agencies, and so forth. Personal details, on the contrary, such as name, weight, age, and sex are kept in medical records as attributes, which need to be kept away from intruders and attackers and should be privately stored. For privacy-preservation, some techniques are applied in the proposed waiver- RBAC and ABAC, which form a mitigating approach called RABAC. Access matrices alongside RABAC are used in designing a framework for improved electronic health record preservation.

Keywords: Data security, Electronic hospital record, ECC, Blowfish, Access Matrix, RABAC.

I. INTRODUCTION

Cloud computing consist of resources matters, service types, and infrastructure types. It is a big data warehouse where computations, operations, and ease of service provision on demand are carried out. Cloud is a forthcoming in this technology setting that takes care of the changing skull trends. It is flexible, cheap, and advantageous to use. The security policies of cloud have been studied in the introduction for the purpose of data authentication for security. Security and privacy will always pose future challenges for any researcher and writer; these challenges include authentication, authorization, integrity, confidentiality, availability, and privacy. The major concerns arise due to dependence on a third party because there could be a chance of losing data. Bulk data is communicated in clouds, which immediately poses the risk of accessing the data by attackers in cloud. As concluded by the researchers in section two, with demonstrating security requirements in the cloud for the safety of health records, challenges related to enhancing security risk were discussed.

Electronic Health Records or EHRs are a repository of patient records and health information of a person, which are stored in an electronic form. These records can be shared in various healthcare centers via networks and exchanges. EHR data consist of multiple sets of information comprising a patient's medical history; test reports from laboratories; demographic data, i.e., name, age, gender, weight, etc.; as well as personal information relevant to billing, which is contained within an electronic health record.

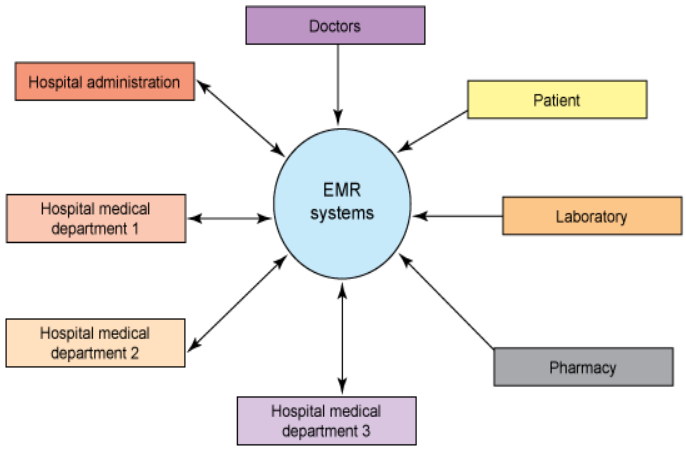

Figure 1: EHR System

Security Concern:

1. **Authentication**

Authentication is one of the security concern in security policies and it cannot be removed ever. Authentication checks user identity and system identity for the purpose of communication.

2. **Confidentiality**

Confidentiality explains privacy; some parameters are required for securing delivery of information to any wrong person by making sure that message will delivered to right person. Only the authorized person have the right to access data.

3. **Availability**

Availability is the important concern due to the maintenance of any hardware. Proper functioning of system requires availability of resources at correct time when required which will save time and cost.

4. **Integrity**

Integrity means accuracy, where data cannot be modified or altered while transmission by unauthorized user. Alteration is the activity where error is created or unauthorized user while transferring of data deletes some sensitive part of the data.

II. RELATED WORK

2.1 Related Work

R.Manoj et al. In[1] contributes the increase in scalability, good fine, grained access control for health record, reduced encryption time and increased security. Author uses security domain for the easy verification of user.

To overcome the limitation of AES, ABE encryption technique is used. AES only works for key length, with the increase in size of data computation time increases. AES is also inefficient for sharing and accessing medical

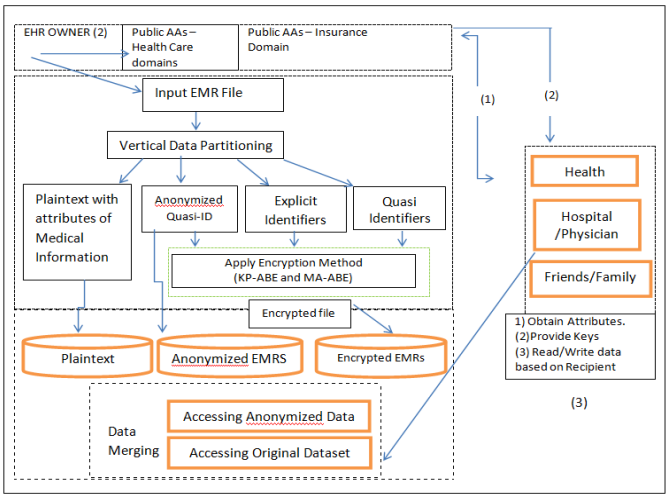

Figure 2: Existing Work by R. Manoj data by user.

III. PROBLEM DOMAIN

Existing work uses Attribute Based Encryption (ABE), where it only works on using different attributes. It is a public key encryption where user secret key and ciphered text are dependent on attributes, attributes like belonging to the place from where he is and which kind of agreements he deals with. In this type of system cipher text is decrypted only when the key attributes matches the ciphertext attributes. It only deals with security in terms of attribute-based encryption, which is resistance to collusion. It means an individual who holds multiple keys can view the data if access is granted by at least an individual key.

It suffers from the issue of key escrow, which means key exchange or key holding by a third party. By key escrow, the key is compromised by some original user of encryption or decryption material with the allowance of returning the original material to its unencrypted state. For cryptographic keys, key escrow also serves as a backup. However, since key escrow requires a third party, it is risky. Another challenge is key revocation, where revocation refers to digital security. With the digital security, internet is managed by the system using security protocol for verifying the management of identity. If certification is taken then it is called as revocation.

Identity of owners and maintainers are transparent in digital certificates. Documents should be authorized and authenticated. Certificate authority manager using security protocols manages digital certificates. If any misrepresentation is identified by certificate authority then people started issuing digital certificates dishonestly. Web users are protected by systems with certificate legitimation. Attribute-based Encryption algorithms are created by Bilinear groups. However, ABE system is created by multi-authorities but with the limitations of instances of cipher text policy.

Without any co-ordination and moments, authorities are set, where simple ABE authority is set by creating its public parameters and provisioning user with private key. Thus, data can be encrypted by user with using attributes and authorities. Full control is maintained with conspire authorities.

IV. SYSTEM ARCHITECTURE

System architecture defines the proposed work through some steps and these steps are cited below as:

- Electronic hospital record data is taken as a dataset.
- On that dataset authentication is achieved using access control techniques ABAC and RBAC.
- Access Matrix with ABAC and RBAC is combined

to achieve RABAC Matrix for access control.

- Electronic medical data is the sensitive data, which needs to be authenticated.
- Roles and attributes are checked by access control for accessing dat.
- Every role and every attribute is checked for the resolution of operations to held.
- This role-attribute table is used for the operation update, that who can access which role and attribute.
- Not every user has approval to access every attribute.

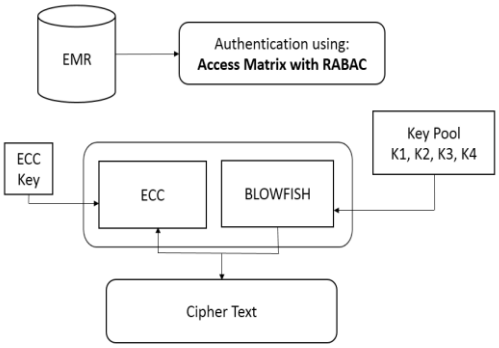

Figure 3: System Architecture

- The study of existing solutions explore that it uses symmetric key cryptographic algorithm for encryption and attribute based access control for rights enforcement.
- Advance Encryption Standards [AES] algorithm suffers with issue of low-key strength due to single key use for encryption and decryption.
- For every role, common permission is granted based on attribute based access control. Likewise, same pattern of cipher text are generated through single encryption iteration.
- ABE experiences the issue of non-existence and non-efficiency. These are the drawbacks for the operations of attributes.
- It has the drawback that it does not determine who will decrypt the data, which is encrypted. This scheme works only for descriptive attributes.
- Access Control matrix has been used to assign rights of individual attribute.

Sample Access Matrix:

1 = True
0 = False

Role: Operator

	Doctorid	Dies is	Investigation	Patient Id	Patient Name
Read	1	0	0	1	1
Write	1	0	0	1	1

Role: Doctor

	Doctorid	Dies is	Investigation	Patient Id	Patient Name
Read	1	1	1	1	1
Write	1	1	1	1	0

Figure 4: Sample Access Matrix

V. RESULT ANALYSIS

Parameter of evaluation is a computation time and is measured for different data size algorithm. Performance evaluation has been made in milliseconds and comparison has been made with previous work. Existing work author has implemented AES algorithm as base algorithm which is replaced by combination of ECC & Blowfish to get better security and strong confidentiality. Proposed work for plain text file size in comparison to AES computation time is represented as graph in figure 5.1 and its table is also designed in Table 5.1. Comparison between presented work and existing work is elaborated below based on file size and computation time and is represented as graph in figure 5.3 and its table is also designed in Table 5.3.

Table 2: Total Computation time for Existing Work

File Size	Computation Time [Existing Work] (ms.)	Computation Time [Proposed Work] (ms.)
1	1593	165
5	4403	689
10	5237	1589
20	6994	3058
50	8750	7589
70	10506	8569
100	12261	10895
150	15752	14528
200	17338	16589
250	19093	18569

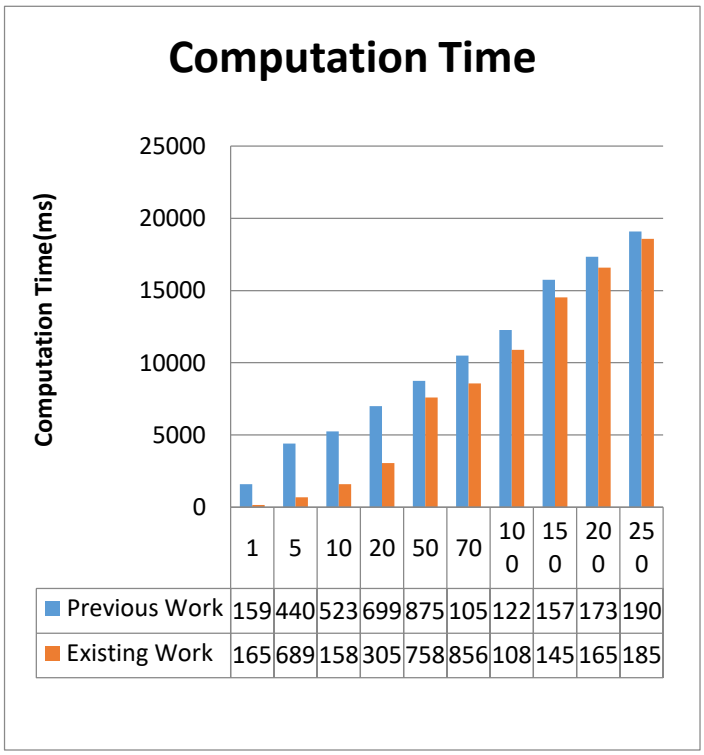

Figure 5: Comparison graph for existing and proposed work

VI. CONCLUSION

The concern for safeguarding and providing privacy to health data dominated this research work. The goal of this project is to protect the credential of the user during communication and while in storage. Here, the EHR has been considered as the dataset and processed through a security architecture to keep the communication safekeeping. For greater efficiency and safety, an association of ECC & Blowfish called public key, and symmetric key-based algorithms to offer confidentiality and authentication during one time has been developed. Security and privacy are major concerns in every field; in the case of outsourced data, the problem becomes even more complicated. Here, a framework is constructed to justify the different layers of security.

The complete work observes certain conclusions, which have written below:

1. There is strong need of security and privacy for to delicate data in cloud.

2. Provided privacy on data while storage using improved AES algorithm, as to avoid information leakage issue.

3. Implement MD5 to maintain originality of data.

4. Two Encryption Algorithm will not only help to improve security level but will also create confusion during cryptanalysis using different cipher text pattern.

Future Work:

1. Image data is acquired for future implementation.
2. In future implementation, AES can be modified by replacing it with a better algorithm for enhanced performance.

VII. REFERENCES

[1]. R. Manoj, Abeer Alsadoon, P.W.C. Prasad, “Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud,” 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering.

[2]. M. N. Shrestha, A. Alsadoon, C. P. Prasad and Houran, "Enhanced e-Health Framework for Security and Privacy in Healthcare". IEEE, pp. 75-79., 2016.

[3]. H. Kumar and H. Gupta, "Cloud Security: An Innovative Technique for the Enhancement of Cloud Security," 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2023, pp. 411-416,

[4]. R. Ranchal, “Cross-domain data dissemination and policy enforcement,” PhD Thesis, Purdue University, 2015.

[5]. S. Suresh, "Highly Secured Cloud Based Personal Health Record Model". International Conference on Green Engineering and Technologies (IC-GET), pp. 1-4, 2015.

[6]. J. J. Yang, J. Li and Y. Niu, "A Hybrid solution for privacy preserving medical data sharing in cloud computing". Future Generation computer systems, vol. 43, no. 44, pp. 74-86, 2015.

[7]. H. Liu, "Data Protection in Cloud Computing Environment: New Dimension of Network Information Security," *2024 First International Conference on Software, Systems and Information Technology (SSITCON)*, Tumkur, India, 2024, pp. 1-5,

[8]. B. Bhargava, “Privacy – preserving data dissemination and adaptable service composition in trusted and untrusted cloud”. NGCRC Project Proposal, CERIAS, Purdue University, Aug.2015

[9]. Y. Chen, J. Lu and J. Jan, "A Secure EHR System Based on Hybrid Clouds". Journal of Medical System, vol. 36, no. 5, p. 3375–3384, 2014. J. Clerk Maxwell, a Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[10]. B. Coats and S. Acharya. S, "Bridging Electronic Health Record Access to the Cloud". IEEE 47th Hawaii International Conference on System Science, pp. 2948-2957, 2014.

[11]. K. Nagaty, "Mobile Health Care on a Secured Hybrid Cloud". Cyber Journals, vol. 4, no. 2, 2014.

[12]. H. Aljafera, Z. Malika and M. Alodibb, "A brief overview and an experimental evaluation of data confidentiality measures on the cloud". Journal of Innovation in Digital Ecosystems, vol. 1, no. 1-2, pp. 1-11, December 2014.

[13]. J. Meyer, "Open SOA Health Web Platform for Mobile Medical Apps: Connecting Securely Mobile Devices with Distributed

Electronic Health Records and Medical Systems". IEEE, pp. 1-6, 2014.

[14]. A. Michalas, N. Paladi and C. Gehrmann, "Security Aspects of e-Health Systems Migration to the Cloud". IEEE 16th International Conference on e-Health Networking, pp. 212-218, 2014.

[15]. J. Reardon, D. Basin and S. Capkun, "Sok: Secure data deletion in Security and Privacy(SP)". IEEE Symposiumon, pp. 301-315, 2013.

[16]. Q. Zhang, M. F. Zhani, R. Boutaba and J. L. Heller, "Harmony: Dynamic Heterogeneity-Aware Resource Provisioning in the Cloud". IEEE 33rd International Conference, pp. 510 519, 2013

[17]. F. Li, B. Luo, P. Liu, D. Lee, and C.-H. Chu, "Enforcing secure and privacy- preserving information brokering in distributed information sharing," IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 888–900, 2013.

[18]. B. Wang, B. Li and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud". IEEE 5th International Conference, pp. 295-302., 2012.

[19]. S. Pearson and M. C. Mont, "Sticky policies: an approach for managing privacy across multiple parties". IEEE Computer, no. 9, pp. 60–68, 2011.

[20]. L. Ben Othmane and L. Lilien, "Protecting privacy in sensitive data dissemination with active bundles". 7th Annual Conf. on Privacy, Security and Trust (PST 2009), Saint John, New Brunswick, Canada, Aug. 2009, pp. 202-213