JES
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

ACCESS CONTROLLED MODEL FOR SECURE MAINTENANCE OF ELECTRICAL HEALTH CARE RECORDS USING XML BASED STORAGE

[1]Mohammed Harisuddin Zain, [2]Dr. Md Ateeq Ur Rahman
[1]PG Scholar , M.Tech, Dept of CSE, Shadan College of Engineering and Technology HYD, T.S, INDIA
harisuddinzain@gmail.com
[2]Professor, Dept of CSE, Shadan College of Engineering and Technology HYD, T.S, INDIA
mail2ateeq@yahoo.com

ABSTRACT

Cloud-based electronic wellbeing record (EHR) frameworks empower restorative archives to be traded between medicinal organizations, which would be required to be added to enhancements in different therapeutic administrations later on. Be that as it may, as the framework design turns out to be increasingly convoluted, cloud-based EHR frameworks may present extra security dangers when contrasted with existing solitary frameworks. In this way, patients may encounter presentation of private information that they don't wish to uncover. So as to ensure the security of patients, numerous methodologies have been proposed to give, to get, to control, to understand archives given to wellbeing administrations. Currently most existing frameworks does not control or consider extra security factors, for example, encryption and computerized marks. In this paper, we have presented a cloud-based EHR demonstrate that performs characteristic based access-control utilizing XACML (extensible access control markup language). Our EHR show concentrates on security, performs incomplete encryption and utilization of electronic marks when a patient archive is sent to a report requester. We use XML based encryption and XML computerized signature innovation. Our proposed model works proficiently and effectively by sending just the essential data to requesters who are approved for treating the patient being referred to.

Index Terms - Access Control, Data Privacy, Encryption, Digital Signature

I. INTRODUCTION

Recently the advancement of data innovation has made incredible walks in the field of restorative data. So as to oversee a lot of restorative information straightforwardly and cost-successfully, the requirement for electronic medicinal information has expanded, and paper-based account techniques are step by step being supplanted by digitized therapeutic data frameworks [1]. EHRs electronically organizes computerized structures containing the majority of a patient's therapeutic data [2]. EHRs pursue global gauges to guarantee interoperability with the goal that information isn't made and overseen by a solitary medicinal services association, however by different restorative establishment frameworks that permit sharing between different human services suppliers and associations [3] (e.g., clinics, research centres, masters, therapeutic imaging offices, drug stores, crisis offices, and colleges).

The adaption of EHR can assume an imperative job in improving patient security and human services quality. The current EHR framework was developed in a concentrated database condition and medicinal data was put away and was different with regards to emergency clinic frameworks. In any case, this approach brings about mind-boggling expenses because of the underlying development of the framework, foundation learning, absence of talented framework designers, and issues with patient restorative data being incongruent with the frameworks in different emergency clinics. One potential answer for the issues portrayed above has started drawing in huge consideration [7]. That arrangement is an EHR framework dependent on the cloud condition. Distributed computing is overseen by a cloud supplier, which has focal points as far as expense and framework extension when contrasted with existing frameworks [8]. Persistent information can likewise be shared and overseen by different human services suppliers.

In any case, an EHR framework in the cloud condition accompanies extra security issues contrasted with a solitary framework condition since patient information trade happens between the cloud stage and different human services foundations [9]. Patients data may cause security and protection issues since it contains delicate and private information about the patient (e.g., wellbeing status data, arrangement of social insurance, instalment for human services, distinguishing proof of the patient) [10]. This data must be maneuverer carefully on the grounds that its presentation would establish a serious break of the protection of the person. The EHR framework must be intended to ensure security and protection when sharing individual patient data [11].

Access control is essential for ensuring security factors while giving records to wellbeing administrations. Access control implies controlled transmission of patient records to approved specialists. Latest access control frameworks for wellbeing administrations are unbendable because of utilizing Role Based Access Control (RBAC) plans [12]. Besides, extra security issues may emerge because of an absence of thought for different security factors. In this way, so as to structure a safe and adaptable access control framework to secure patient protection, we propose a quality-based access control demonstrate utilizing XACML [13].

The fundamental commitments of this paper are as follows: 1) The property-based access control utilized in the proposed model can give adaptable and fine-grained control when contrasted with existing RBAC plans. 2) Performing fractional encryption of patient security related components in patient reports by means of extensible markup language (XML) encryption [14], the danger of extra protection introduction for the patient when an approved client sees the patient records can be averted. 3) The advanced mark procedure can demonstrate that a record has not been distorted or adjusted, and can avoid non-denial of the report. Furthermore, the proposed model fits in with the specialized shields of the American standard medical coverage compactness and responsibility act (HIPAA) [15].

The rest of this paper is sorted out as pursues. Segment 2 examines the related guidelines and access control ponders for EHR framework improvement. Segment 3 presents a two-stage show for building up a protection safeguarding EHR framework. Section 4 depicts the model execution of the proposed model dependent on real restorative information. Section 5 demonstrates the consequences of the correlation between the current investigations and the proposed model regarding security angle. Section 6 give conclusion and future work.

II. RELATED WORK

A. Standards for EHR Systems

There are as of now a few guidelines being developed for indicating EHRs, for example, HIPAA, OpenEHR [16], the Health Level 7 (HL7) Clinical Report Design (CDA) [17,18], and Congruity of Consideration Document (CCD) [19]. HIPAA gives safety efforts and security insurance components to ensure wellbeing data. HIPAA has characterized individual recognizable data (e.g., government disability number, medicinal ID number, Mastercard number, driver's permit number, place of residence, phone number, therapeutic records, and other vital data) as ensured wellbeing data (PHI). HIPAA was made to ensure the person's PHI. In 2009, HIPAA was redesigned into wellbeing data innovation for monetary and clinical wellbeing (HITECH) [20]. HITECH gives extra consistence gauges to organizations engaged with social insurance. The specialized protect bit of HIPAA indicates what necessities must be met in the structure of access control, transmission security, and so on when creating therapeutic frameworks.

The HL7 CDA is a markup standard that characterizes the semantics and structure of CDA clinical reports for sharing purposes. Clinical documentation is a record of therapeutic perceptions and administrations, and CDA records may incorporate content, pictures, sounds, and another interactive media content. The CDA is encoded in XML, and an execution framework that trades CDA archives must meet every single lawful necessity for verification, privacy, and maintenance of records. Since the CDA was affirmed as an American national benchmark organization (ANSI) standard in 2005, the HL7 panel has concentrated on making reusable formats and requirements for generally utilized clinical documentation. For interoperability of restorative information, American Society for Testing and Materials (ASTM) built up progression of Clinical Consideration Record (CCR) [21] and HL7 affiliation set up CCD standard by joining HL7 CDA and CCR. These guidelines express close to home wellbeing data dependent on the XML language.

Open EHR is intended to empower interoperability of wellbeing data between EHR frameworks (or inside an EHR framework). Open EHR is a steady model that has been utilized for more than 15 years and is uninhibitedly accessible to anybody, whenever, anyplace with an open permit. Not at all like the customary EHR advancement demonstrate, in light of the fact that the specialized reference show is totally isolated from clinical learning utilizing a two-level data display, the specialized part can be structured by architects, and the clinical learning bit can be planned by clinicians.

B. Privacy-preserving Approaches for EHR Systems

Numerous survey papers have reviewed and carefully examined privacy-preserving schemes for EHR systems [12, 22-27]. Abbas as well as Khan [12] described the requirements which should be considered for privacy in an E-health cloud. To preserve health data privacy in a cloud environment, they described how the e-Health system should consider the following

requirements: integrity, confidentiality, accountability, authenticity, audit, non- repudiation, unlinkability and anonymity. They also assessed how well studies on privacy preservation in EHR systems consider these factors. They classify privacy-preserving approaches in e-Health Clouds as cryptographic approaches and non-cryptographic approaches. The cryptographic approaches uses encryption schemes like attribute-based encryption (ABE) ,public key encryption (PKE) and symmetric key encryption (SKE) to protect health data in e-Health Cloud environments. Studies classified as non-cryptographic approaches mainly use techniques such as policy-based access control. Oleshchuk and Pussewalage[22] classify technologies for privacy preservation into various cryptographic mechanism approaches (e.g., PKE, ABE and SKE), access control approaches (e.g., RBAC, ABAC), and biometric approaches. They classify the security and privacy requirement elements for e-health as a patient's understanding, a patient's control, confidentiality, data integrity, consent exception, non- reputation, and auditing. Then, they assess whether papers proposing privacy-preserving schemes reflect these factors. Fernández-Alemán et al. [23] selected the top papers in the field and analyzed the latest research trends. Their results shows that more than half of the EHR systems using access-controlling use RBAC, and that 22% of them uses a public key infrastructure (PKI)- based digital signature mechanism.

III. EXISTING SYSTEM

Cloud-based electronic wellbeing record (EHR) frameworks empower restorative archives to be traded between therapeutic institutions. Cloud-based EHR frameworks might present extra security dangers when contrasted with existing solitary frameworks.

Hashing Algorithm is the method utilized in the current framework. A hash calculation or hashing is a capacity that changes an information string into a numeric string yield of fixed length. The yield string is commonly a lot littler than the first information. Hash crashes are basically unavoidable when hashing an arbitrary subset of an expansive arrangement of conceivable keys. Hash tables become very wasteful when there are numerous impacts.

Disadvantages of Existing System:

- Hash collisions are practically unavoidable when hashing a random subset of a large set of possible keys.
- Hash tables become quite inefficient if there are many collisions.

IV. PROPOSED SYSTEM

We propose a cloud-based EHR display that performs property-based access control utilizing Extensible Access Control Markup Language (XACML). Our EHR show is majorly concentrated on security, performs fractional encryption and even utilizations of electronic marks when a patient report is sent to an archive requester. Encryption Algorithm is the procedure utilized in the proposed framework, which is explained underneath:

It is a numerical method for performing encryption on information. Using a calculation, data is made into inane figure message and requires the utilization of a key to change the information again into its unique structure.

Advantages of Proposed System:

- An encrypting algorithm scrambles the message and it can only be unscrambled with a key created at the same time.
- Cipher algorithms are either symmetric or asymmetric for encryption security. For example: Symmetric - the exact same key is used to encrypt and decrypt data.

V. THE PROPOSED EHR SYSTEM MODEL FOR PROTECTING PATIENT PRIVACY

In the proposed EHR show, ABAC utilizes XACML and XML security for encryption and computerized marks is utilized to ensure persistent protection. This can shield patients from the danger of security encroachment by giving just the required substance from the mentioned patient medicinal archives to approved clients.

A. FRAMEWORK

We propose a new methodology for the development of an EHR system that protects the privacy of patients in a cloud environment. In this project we have the following modules.

1. User Interface Design
2. Electronic Health Record System
3. User
4. Admin

1. User interface design:

This is the primary module of our task. In this, the application client's initially make their record legitimate which are put away at the back end for confirmation or for giving security to the records. On the off chance that client needs to get into his record, first they need to present their imperatives, for example, username, secret key, etc… without which he can't get to the record. In our task as indicated by activities they are performing; we scatter the clients as administrator or typical application client.

2. Electronic Health Record System:

Cloud-based electronic wellbeing record (EHR) frameworks empower therapeutic reports to be traded between restorative foundations; this is required to add to upgrades in different medicinal administrations later on. In this undertaking the electronic records are put away in xml documents and are stored as encoded xml records to server.

3. User:

The outsider clients have the authorizations for looking through the information identified with electronic records. To see the information, the client must need a key to decode a document because of which we are putting away the documents as encryption in cloud. Also, the keys are put away at administrator, So when we need a document information we need to get key from the administrator, for that we have to send key solicitation to administrator for specific record.

- Register
- Login
- Searching records by keyword based
- Select record
- Send record key request for admin
- Get record key from admin
- View the record data by decrypting that by using key
- Logout

4. Admin:

Here the administrator will deal with entire site. The administrator will include the electronic wellbeing records into cloud, when he transfers the records, he get a key. The administrator also needs to keep up the key with clients to unscramble the record.

- Login
- Upload records
- View user key requests
- Give response (Accept/decline) to the user key request
- View records details

He had his unique username and password apart from those he can't be able to perform any operation because he can't get into his home page where these operations are maintained.

B. GIVEN INPUT EXPECTED OUTPUT

1) User Interface

Input: Enter login name and password.
Output: If valid user means directly open the home page otherwise show the error message and redirect to the registration page.

2) Admin upload record

Input: Give record details and data.
Output: If record was successfully uploaded the admin will get record key as well as successful message. Otherwise he will get error message.

3) User searching by keywords

Input: User will enter keywords related to record
Output: The user will get related records depending upon keywords which are entered by user.

4) Key requesting and responding

Input: User send key request to admin
Output: Admin will send particular key to the user to decrypt the file.

5) Decrypt record

Input: Enter a record key and click decrypt
Output: If the user entered a valid key of particular record, the record will be displayed in the form of decrypt otherwise the user will get null data.

C. TECHNIQUE USED OR ALGORITHM USED

Since the genuine EHR framework is extremely huge, there is a farthest point to the execution of the framework in this examination. In this manner, we limit the contribution of client prerequisites so as to streamline usage intricacy. For instance, a client may choose just a constrained arrangement of records or activities. This likewise improves the errand of complex approach structure. The key administration required for encryption and marking likewise utilizes a neighbourhood key store so as to decrease usage intricacy. presents the UML arrangement chart of the executed framework.

For instance, if the arrangement is for an archive in the medicinal classification, we can indicate the objective of the strategy as pursues:

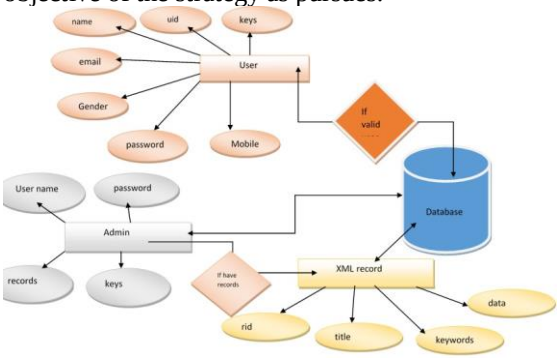

Fig 1: E-R Diagram

An arrangement can indicate different tenets. Guidelines comprise of a Target, at least one Conditions, and an Effect. The objective component utilized in the standard is utilized to assess whether the comparing rule is identified with the solicitation as the objective of the arrangement. It is utilized to assess if the standard is identified with the solicitation. In the event that no objective is indicated, the standard is assessed for all solicitations. Conditions indicate approval rationale proclamations that contain Boolean articulation esteems. The standard is utilized to decide whether the condition is valid or false (or Indeterminate).

The impact esteem is a component that figures out what esteem the standard will return when the Condition is valid. For instance, you can determine the accompanying model standards for the Policy precedent above.

On the off chance that the condition is valid and the impact esteem is grant, at that point the arrival esteem is grant. An Obligation is a discretionary component that permits XACML to empower all the more fine-grained get to control. Commitments determine the activities that the PEP ought to uphold while implementing approval choices.

In XACML, every approach set has various strategies, and every strategy has different guidelines. A contention can happen when distinctive outcomes are produced from each related approach or guideline. This issue can be settled by utilizing an approach or principle mix calculation. In case of a contention, the blend calculation is utilized to rank the aftereffects of every arrangement or rule and infer the outcome. Table 1 introduces the standard blend calculations bolstered by XACML 3.0.

So as to determine setting, a solicitation message in XACML utilizes a structure indicating trait classifications, characteristic qualities, and metadata. Fig. 2 shows the structure of a XACML demand. As delineated in the figure, one solicitation message comprises of a few qualities, and traits are involved four classifications: subject, asset, activity, and condition. The solicitation message asks the PDP the accompanying inquiry: For a given subject, is it permitted to play out the predefined activity on the predetermined asset in the predefined condition? In the event that the solicitation message fulfils the strategy condition, it restores the Effect esteem

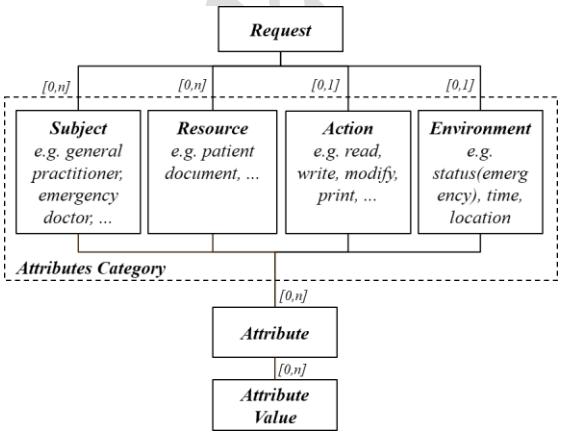

Fig 2: Structure of an XACML request

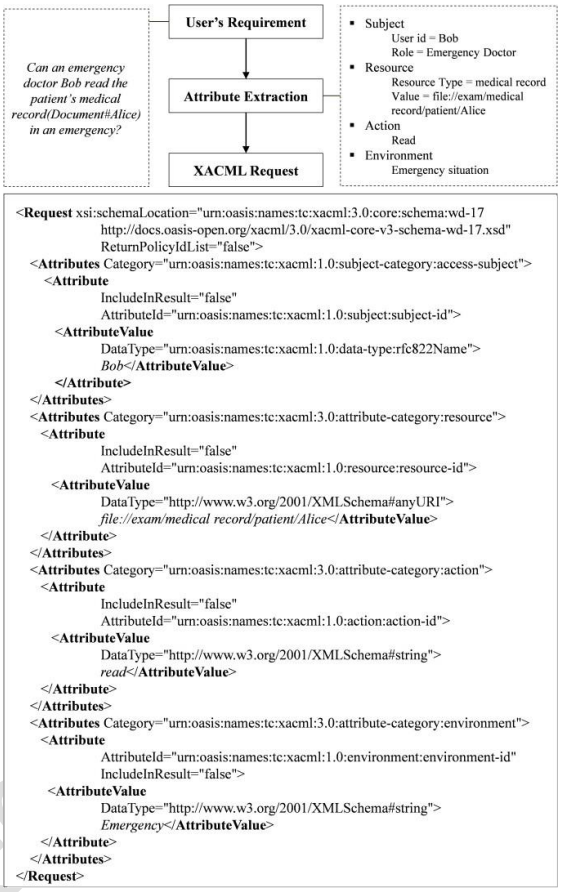

Fig. 3. An example of the process of generating an XACML request message in a scenario where the emergency doctor Bob accesses patient Alice's data in an emergency.

performed in the PEP and the created XACML demand is sent to the PDP to assess whether it is approved. In this precedent, as a prerequisite of the client, the crisis specialist, Bob, sends a solicitation to peruse the restorative reports of the patient, Alice, amid a crisis. At the point when such a necessity is made, a property extraction process is performed to concentrate and match the qualities from the prerequisite. To begin with, the performing artist, Bob (all the more explicitly Bob's id), needs to get to the reports coordinating the Subject. The archive that Bob needs to get to is coordinated utilizing the asset data. The asset type is a therapeutic record, and the esteem is the way to the archive. On-screen characters can perform different activities on the report, for example, read, compose, and print. In this precedent, just read is permitted, so the read credit is coordinated to the Action quality. At long last, the Environment coordinates the crisis circumstance. Toward the finish of the property extraction access, a XACML demand message will be produced following the expansion of a solicitation header and trait metadata data input.

Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

The XACML demand message produced by the PEP is passed to the PDP and assessed for endorsement. Fig. 4 is a stream graph delineating the way toward getting a solicitation message from the PEP and performing assessment. This procedure can be isolated into three phases. The primary stage is the way toward deciding similarity settings and performing preprocessing preceding assessing the solicitation explanation. For instance, the way toward characterizing XACML run constants is incorporated this progression. This enables the PDP to appreciate the importance of the predetermined information esteems while investigating the substance of a solicitation message.

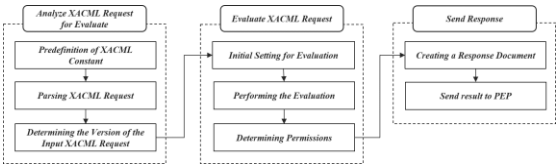

Fig 4: The process of analysing the request message and performing the evaluation process by the PDP to determine whether the user is a user who can access the patient's document.

This procedure is performed before the solicitation message is acknowledged, and is fundamental for deciding whether the got solicitation message is legitimate. At the point when the legitimacy of the solicitation message is confirmed, the PDP parses the solicitation explanation to remove the ideal data. Since language structure is somewhat unique relying upon the adaptation of XACML, one should make sure for compatibility via version checking and use an suitable evaluation technique based on the version.

VI. RESULTS

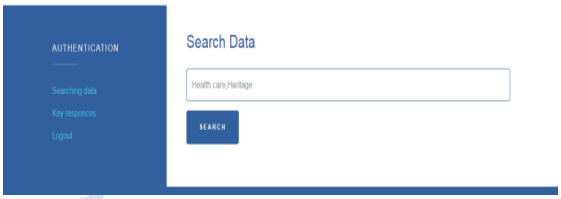

Fig 1: Search Page

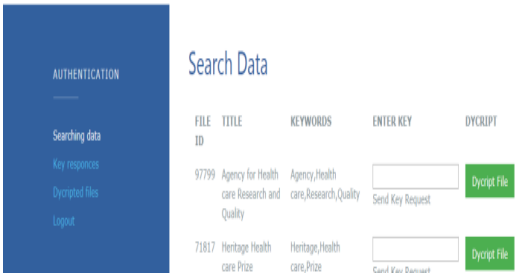

Fig 2: Search Result Page

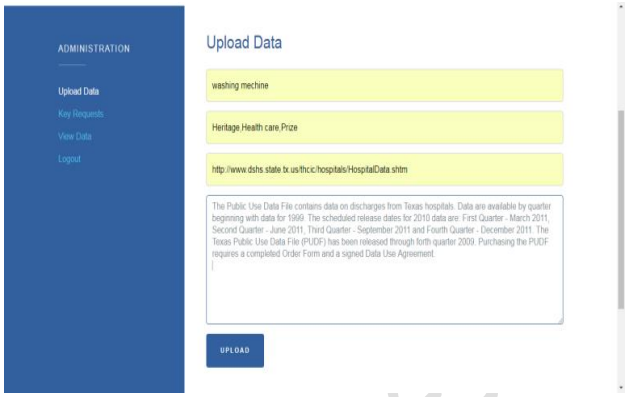

Fig 3: Admin Upload Page

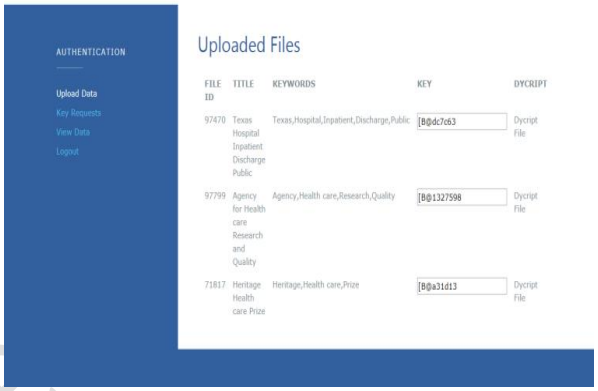

Fig 4: Admin Uploaded Files View Page

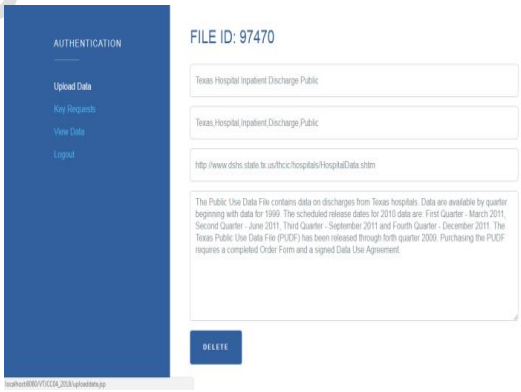

Fig 5: Results Page

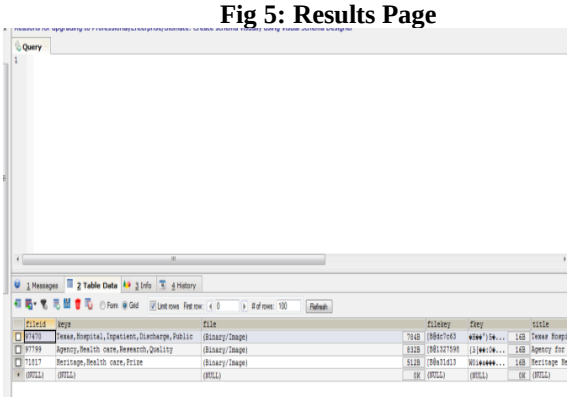

Fig 6: Database Structure

VII. CONCLUSION

As of late, EHR frameworks in the cloud condition have appeared potential to improve the nature of therapeutic administration by sharing and using persistent information crosswise over different restorative foundations. Be that as it may, this condition makes extra security dangers and patient protection can be abused by different pernicious assaults. Not-withstanding the significance of information security, numerous frameworks don't consider security factors amid their demonstrating procedure or view them as minor elements. We proposed a cloud-based EHR show that ensures tolerant security. The proposed model is partitioned into two phases: Get to control, and the utilization of encryption and advanced marks. The proposed model uses an ABAC strategy based upon XACML. In the wake of performing access control on patient reports, encryption is performed and computerized marks are included utilizing XML encryption and XML advanced marks as an additional safety effort. The proposed model gives more adaptable and fine-grained control than existing RBAC frameworks and lightens the danger of uncovering quiet security data by utilizing fractional encryption and electronic marks. The execution of a model showed the plausibility of the proposed model. We contrasted the actualized security factors and those utilized in other related examinations and established that the proposed technique is better than past strategies as far as security. Later on, we will additionally refine the procedures utilized in the proposed model and execute extra security highlights. We will likewise extend the execution of the model to actualize a progressively refined framework and perform quantitative execution assessment.

REFERENCES

[1] Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. Journal of the American Medical Informatics Association,

[2] van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter- organizational future proof EHR systems: a review of the security and privacy related issues. International journal of medical informatics

[3] Tang, P. C. (2003). Key capabilities of an electronic health record system. Washington, DC, Institute of Medicine of the National Academies

[4] Miller, R. H., West, C., Brown, T. M., Sim, I., & Ganchoff, C. (2005). The value of electronic health records in solo or small group practices. Health Affairs.

[5] Middleton, B., Bloomrosen, M., Dente, M. A., Hashmat, B., Koppel, R., Overhage, J. M., ... & Zhang, J. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. Journal of the American Medical Informatics Association.

[6] Simon, S. R., Kaushal, R., Cleary, P. D., Jenter, C. A., Volk, L. A., Poon, E. G., ... & Bates, D. W. (2007). Correlates of electronic health record adoption in office practices: a state wide survey. Journal of the American Medical Informatics Association.

[7] Ratnam, K. A., & Dominic, P. D. D. (2012, June). Cloud services- Enhancing the Malaysian healthcare sector. In Computer & Information Science (ICCIS), 2012 International Conference

[8] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference.

[9] Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009, Nov.). Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud computing security.

[10] Ray, P., & Wimalasiri, J. (2006, Aug.). The need for technical solutions for maintaining the privacy of EHR. In Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE.

[11] Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy- preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics.

[12] eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS Standard, 22 Jan. 2013,

[13] XML Encryption Syntax and Processing, W3C Recommendation, 10 Dec 2002.

[14] Standards for Privacy of Individually Identifiable Health Information: Final Rule. Dec. 28, 2000.

[15] openEHR Community: openEHR,

[16] HL7: Health level 7 (HL7),

[17] Dolin, R.H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F.M., Biron, P.V.: Hl7 clinical document architecture, release 2.0. ANSI Standard (2004)

[18] C 32 - HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component.

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

[19] HITECH Act enforcement interim final rule. US Department of Health and Human Services. 2013

[20] ASTM E2369 - Standard Specification for Continuity of Care Record (CCR).

AUTHOR's PROFILE:

MOHAMMED HARISUDDIN ZAIN, Software Engineer in a reputed organization and along the way pursuing M.Tech from a JNTUH affiliated college. Previously received a B.E Degree from Osmania University affiliated college in the year 2017 and have done the specialization in Computer Science Engineering. I have also published and leaded a research work named "Energy Efficient and Reliable Routing Protocol in Wireless Ad Hoc Network" previously in the field of Networking.

Dr. MD ATEEQ UR RAHMAN, received the B.E, M.Tech (CSE) and Ph.D.(SIT) degrees from Gulbarga University, Visvesvaraya Technological University and Jawaharlal Nehru Technological University Hyderabad, INDIA respectively in 2000, 2005 and 2014 respectively. He has vast academic and administration experience and has worked under various capacities as Assistant Professor, Associate Professor and Professor in Different Engineering Colleges from 2005 to till date. Presently he is working as Professor and Research Coordinator in Computer Science & Engineering Dept, Shadan College of Engineering & Technology, Affiliated to J.N.T.U.H University, INDIA. His research areas of interest include Spatial Data Mining, Image Processing, Cloud Computing and Computer Networks etc.