International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Assessing Threats and Vulnerable Attacks of Health Care Data in Cloud-Based Environment

L. Abirami, J. Karthikeyan

Abstract: What: ***Healthcare industries have been unified with the advent of cloud computing and Internet of Medical Things in recent past. How: As simplicity in access and transfer of medical reports increased, so does the impact of losing potential information. Adopting a cloud environment has eased the work of medical practitioners and provided world class medical attention to patients from remote corners of a nation. It has added the responsibility of cloud service providers to improvise the existing standards for protecting information in a virtual platform. A number of benefits not limitedto universal access, advice from renowned medical experts for deciding on diagnosis plan, alerting patients and hospitals in real timeand reducing the workload of labor are achieved by cloud environments. Hospital Information Systems (HIS) are the evolved data forms maintained manually in medical institutions and they are preferred in a cloud platform to improve interoperability. The information carried in such medical systems possesses critical information about patients that need to be protected over transmission between independent environments. This becomes a mandatory requirement for designing and implementing an access control mechanism to identify intention of users who enter into the environment. Relaxations in access control architectures will compromise the security of entire architecture and practice. Why: Intention - Demand Tree is proposed in this paper to limit the access rights of users based on their roles, requirements and permissions to monitor the usage of Health Information Systems. Investigative results illustrate that the risks of losing credible information has been limited and convenient than previous standards.***

Index Terms: Public Healthcare, risk analysis, access control, privacy, information systems

I INTRODUCTION

Advancements in technology have converted the manual systems of recording information of patients' into digital format. This digital information is made available to every practitioner with the right credentials and access rights. The systems are classified into Hospital Information Systems (HIS) comprising general and personal information of a patient, Laboratory Information Management System (LIMS) holding information about patients past and present health conditions, Picture Archiving and Communication Systems (PACS) which carries reports from various medical equipment's in a digital format, Radiology Information System (RIS) managing medical imageries and Electronic Medical Record Systems (EMRS) having information of progress and regress of diagnosis for each patient. Other information which is considered to be credible is details of banking and transactions, concessions availed from governmental and insurance sectors, details of friends and guardians [1] etc. These records will be transferred over reliable communication medium between healthcare institutions for further treatments and medical opinions from experts around the world. Cloud environments will try to mandate as much information to be retrieved and stored to facilitate optimizations and reduce communication costs. The information required for proper and quick medical care is also gaining attention by cyber attackers and architectures of hospitals are currently under threats [2]. Yet the cloud environments are coming up with counter measures to overcome the attacks and protect information. In 2017, according to the statistics of HIPAA Journal, nearly 370,000 records are manipulated and 77% of information is stolen. Stealing credible data about patients and their conditions for ransoms, misuse and compromising the strength of an institution for affecting the reputation from competitors are some of known impacts of such criminals. Cloud computing has simplified intense processes in medical institutions and acts as a one end solution for ensuring timely treatments with enhanced quality and cost effectiveness. When an information system is designed, measures to protect data are the primary concern in these applications. The system cannot omit any data which are significant to understand the condition of patients, reaction to previous treatments, allergies and much more. Giving access control strategies along with other design factors is one among the fruitful solutions for problem in question. Many researchers have conducted their research in securing an architecture that holds private and personal information of patients [3]. They have justified the need of implementing a platform universally for interoperability without which the processes will take considerable time [4]. The cost of a highly protective environment is also high that led us to no other choice but cloud computing. Since the entire risk of sharing information and losing it to criminals are mapped to hospitals, patients will not bear any responsibility. Unlike cloud solutions as architecture, platform or service for other industries, medical institutions demand more counter measures over data breaches. Commonly offered services by a cloud service provider are ease of access of data and flow of control, supporting multiple formats of data in structured or unstructured backgrounds and a user friendly virtualization.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Abirami. L, she received his UG and PG degree in Computer science discipline.
Karthikeyan J, Assistant Professor in School of Information Technology and Engineering, VIT, Vellore.

These services are important for other clients but for a medical institution, it seeks more. We adopt Infrastructure as a Service (IaaS) model in this paper to devise a framework with access control strategies to protect patient information. The primary concerns in this model are to optimize the flow of data to and from medical institutions, securing information by limiting access rights based on user profiles, highly competent, strong Infrastructure and finally monitoring the risk and reporting them for necessary actions [14][15]. The valuable information is categorized in following segments to understand where the designers should pay more attention and the impact of each attack over medical records is documented. Those risks are analyzed for their origin and a corrective approach is recommended in each category. To enhance security of the proposed model, an access control strategy is defined and tested against commonly known threats. The model intends to address the deficiency of previous approaches in identifying the normal operations of a hospital staff, procedure and other works clinically. Risk management is an inevitable factor that has to be included when a cloud environment is adopted by a medical institution. Provided with risk management strategies and access controlling mechanisms, this model will be a secure solution for this industry.

II BACKGROUND STUDY

The study begins with identification of significant records that constitute the information maintained in a medical institution. The diversity of records possesses critical importance based on the credibility of information retrieved from patients. The following table 1 shows the names of records and their importance levels [16].

Table 1: Significance Values of Hospital Records

S.No	Name of Record	Significance
R1	Reputation of Hospital	Highest
R2	Belief among patients	Highest
R3	Cooperation of Staff members	Higher
R4	Movable & Immovable Assets	Highest
R5	Personal Information – Sensitive	Highest
R6	Personal Information – Normal	Higher
R7	Personal Information – Health	Higher
R8	Human Resource Information	Higher
R9	Availability of Service – Emergency	Highest
R10	Availability of Service – Normal	Higher
R11	Access Control	Highest
R12	User Credentials	Highest
R13	Physical Devices	High
R14	Cloud Service Interface	Highest
R15	Communication Interface	Higher
R16	Application Interfaces	High

ENISA guidelines are followed in deriving the important records to be maintained in a medical institution. Each record will be having a significance value categorized into High, Higher and Highest. This paper registers all records in a hospital to be potentially important since they cannot be revealed at any cost to a cybercriminal. After the records to be maintained securely, the list of possible threats are determined. The table 2 highlights the different threats which are prone in a cloud environment. It also maps how the hospital records are subjected to respective threats.

A. Classification of Threats

The threats [17] in a cloud environment are explained with reference to Cloud Security Alliance (CSA). *Illegal Entries for Data* may be performed knowingly or unknowingly even by authenticated users sometimes in following Table 2.. Information stored in cloud platform is identified as potentially important which should be protected at all times. Users who utilize the system may decide to retrieve that information for releasing into insecure environments for personal gain. When a person who specifically has no intention or purpose to visit a patient profile, his/ her transactions details, address or process that for a different purpose is termed as a breach. This illegal attempt will lead to unethical usage of revealed information in some other means. There are times when the right users may forget to log out their accounts. The subsequent user gains access to previous user's account. *Manipulated Information* is a process of disturbing the original contents in a patient's record either by deleting, corrupting or changing the meaning of contents. This process may be carried out manually or automatically by software procedures. Most recently, many companies were affected by ransomware viruses which gained access to information stored in renowned companies. This manipulation may occur while storage or transmission from one location to another. The permissions granted to different users of the architecture should be limited to prevent attacks of this category. The accounts may be *illegally possessed* without the knowledge of right users. The architecture believes that the right user is accessing the information and the rightful user has no idea of what is happening inside the system. Any misleading email or downloads may trigger the process of gaining access rights over the right users. The attackers impersonate the rightful users to create a safe approach to steal information.

Table 2: Threats and their Classifications

Threats	Type	Records Affected	Category
T1	Illegal Entries for Data	R1, R2, R4,R5,R6,R7	Loss to Information
T2	Manipulated Information	R1,R2,R5,R6,R7,R12	
T3	Illegal Possession of Accounts	R1,R2,R5,R6,R7,R12	Loss to integrity of communication mediums
T4	Insecure Entry Points	R1,R2,R5,R6,R7	
T5	DoS Attacks	R1,R2,R9,R13	
T6	Compromised Users	R1, R2,R3, R4,R5,R6,R7,R8	Loss due to cloud adoption
T7	Misuse of loop holes in architecture	R1,R2,R6,R7	
T8	Improper design	R5,R6,R7	
T9	Trust based sharing of credentials	R1,R2,R6,R8,R9, R10, R13	

All cloud environments provide a user friendly Application Program Interface to facilitate a one point entry for configuration of the system, managing users, interactions and monitoring of the system from a single point of view. These are defined entry points on which the entire security of a cloud platform is relying on. When a cloud platform is deployed for a client, predefined configurations and recommendations to improve the security is given along. When the end users decide to ignore those recommendations, the system opens the chances for illegal entries or gaining access to these APIs. One time access through this *insecure entry points*by a well-equipped attacker may change the entire security configurations. *Denial of Service Attacks* is a commonly known attack in all types of networks, where the intended services to the rightful user is blocked by invalid or suffocating number of requests initiated by attackers. The time taken by a server to validate and distinguish original and attacked packets by a server will be so long that users will continue to wait for an infinite time. The acknowledged messages by the server will not reach the address defined by the attacker as they are randomly generated. Server might continue sending the acknowledgements without terminating the connection. Once the server decides to terminate the connection after the threshold time, more number of requests is generated by an attacker with a different/randomly generated address. Time taken for resolving this issue is long enough to prevent the original service for which the server is designated for.The attackers of a domain need not be external in all cases. The registered loyal users may be *compromised* to misbehave and function against the norms of an organization. Former or existing employees may be lured to promises and made to betray the management. They may work along with hackers to provide sufficient access to steal information in all areas like data, systems or networks. A design cannot be 100 percent perfect especially in terms of software. The cloud architecture designed and implemented for a hospital domain may have a number of *loop holes* that will be points of entry to cyber criminals. This is due to negligence of some important terminologies when *design* is planned. Improper design will attract hackers to misuse the availability. The loss of data may not be visible until some credible information is stolen from the platform. The habit of sharing passwords and important features that permit secure login is common in friends and family. This is another potential threat in cloud computing. Even one time passwords which are sent to individual phone numbers are sometimes shared. We are now prone to phone calls asking our one-time passwords and a huge scam is operating in the dark world. The users do not take this security option seriously in most of the times. This has also permitted the hackers to target the weaker section of society to claim that they are calling from reputed organizations and retrieve the information meant to be protected. *Credentials* must not be shared in any cases.This model investigates the practical advantages of introducing Role Based Access Control in allocating permissions to users of a cloud environment. The information systems will be defined with regular list of users each holding a number of access rights. When a new user is registered in a system, their designation will be deciding their access rights automatically rather than manual assignment. In Hung et al [5] approach, demand of protecting the privacy of patients especially in a electronic means of maintaining data mode is advocated. The approach also handled information based on their importance and segregated them according to their display to users. Irrespective of permissions, some data will be protected against viewing by private officers [6]. Big Data application has simplified the terms of managing huge voluminous information available in medical institutions. This technique has also improved performance and security of the applications. Personal Health Records monitored electronically has reduced the worries of patients from illegal transfer, leakage and loss in some cases. As the simplicity is experienced, many hospitals have started to adopt cloud computing solutions. Hsu et al [10] devised a framework to assign permissions to users based on their roles played in that organization. Ontology and semantic modeling is absolutely necessary to perform these permission assignments automatically. Gritzalis et al [7] researched in assessing the risks associated with patients and their privacy when their data is shared in a common platform. Rostad et al [8] suggested that the problem is unavailability of enough facts to distinguish information based on their relevance. All these mentioned models have been working based on the roles and associated access rights. The systems may use the knowledge of medical industries and semantic approaches to assist with better performance of applications and interfaces. In Lee et al [9]

design of health records and sharing platform between independent medical institutions namely Integral Healthcare Enterprise-Cross Platform Document Sharing, W3C ontology language is used for updating information in Personal Health Records. Personal diseases were managed and collated by health resources available in World Wide Web. Information stored in medical records has elevated the chances of knowledge discoveries and the overall performance and quality of such applications have improved to new heights. Associations between diseases, their effects, symptoms have been transformed into knowledge in International Classification of Diseases and Systematized Nomenclature for Medicine- Clinical Terms. Beimel et al introduced the conceptual model to retrieve knowledge from incoming requests originated from new users. Li et al. defined a strategy to relate the concepts and instances provided in system after enforcing an authorization portal. The healthcare systems have been introduced as business models in Blobel et al [11] technique with the effects of care paradigms to enhance accuracy and control. A semi automatic model was designed by Gordono et al. [12] to reduce the participation of medical experts to produce a knowledge set from available information. This model was also cost effective. This overture intends to analyze the performance and security after incorporating risk analysis, monitoring and preserving the privacy of patients in a globally exposed environment.

III INTENTION – DEMAND TREE MODEL FOR ACCESS CONTROL

The objective of this model is to analyze and distinguish users in the automated health system based on their participation in a hospital. Roles along with information about their intention and demand will generate a tree for identifying the areas to be given access to. Many information systems have provided access to many individuals who do not possess any relationship with the operations with patient data. Unnecessary disclosure of patient information will be prevalent if such cases are reported [13]. To eliminate this problem, a model for justifying intention and demands will be deciding on which access rights, a user is facilitated with. The rightful user will be assigned with a default role to play in the automated system. For understanding, the roles are determined as doctors, nurses, administrators and finally patients. Each user will be permitted with a respective set of rights within the system. The intention component will decide if the user has appropriate permission to access certain rights, and hands over the request to demand component. Demand component will identify the real necessity of handling such data and verify the user intention. Upon successful verification, requesting user will be delivered with appropriate information.

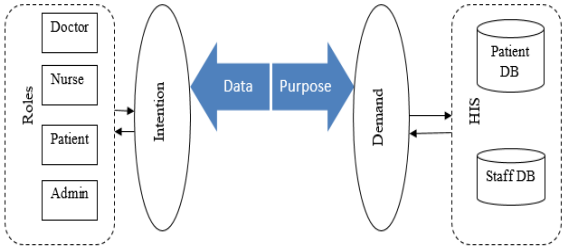

Figure 1. Architecture of Intention –Demand Tree Based Access Control Mechanism

Better control over the information in HIS is achieved through this approach. In a normal system, role based access rights will be given. If a doctor intends to view records of patients' health records, his/ role is already entitled to view without any restrictions. Similarly, administrators may decide to view any patients and their related information without a trace in the system by overriding some source codes. This approach has the intention of every role stated in the intention components. When a user wants to access the files for which they do not own rights, the demand component will act and provides necessary workflow and criteria to be satisfied. Upon justification of the demand, they will be provided a temporary access to demanded list of patient information. The intention of a user cannot be identified easily as they are decided by individual human beings. Intention stated in this architecture denotes the purposed visit of one user into the system. Every access into the system will be returning some information to the claiming users. Such retrieval should carry a relationship derived between intention and demand.Intention – Demand Tree model intends to generate a relationship map between intentions of patients and the information inquired about different users. This approach will deliver a specific control over the users and permissible information. This tree is a significant process in this approach. In a diversity of processes, many participants like doctors, medical technicians, nurses seek the system for necessary information of a patient. This is termed as the intention of users who seek the system. With each branch of the tree, intention gets more specific and users are limited to minimal number of files. The following figure 2 illustrates how each levels of intention are described in the system. This tree will narrow down the exposure of details to individual users even with intention of mishandling information. When a user tries to break in, the system will present with a number of questions to analyze the intention and observe the demand. This presentation will also limit the access to all available information within the HIS. Right users will be directed to demanded list of files and provided with access control to certain domains.

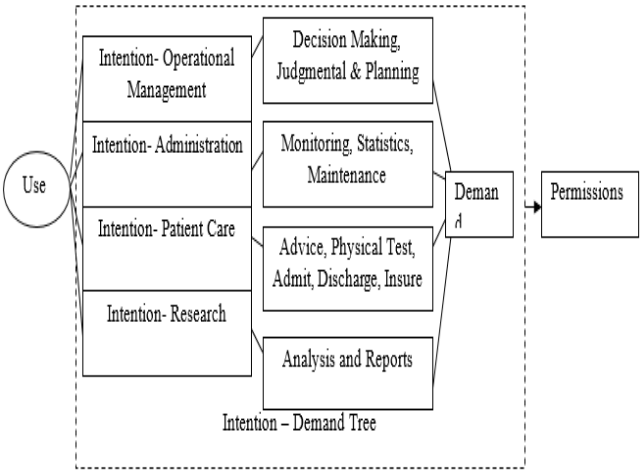

Figure 2. Intention – Demand Tree

The illustrations given in the above sections explain the functional model to determine the permissions for accessing medical records in HIS after knowing the intentions and demands of a user. Two methods are used for this approach, one to identify the intention and other to define permissions. These two approaches are explained algorithmically in the next section. The exact purpose of visit will be determined in first approach.

Algorithm: Intention – Demand Tree for Deriving Permissions

Input: Users U, Roles R, Intentions I.

Output: Permissions based on input URI

1) Let $i_1, i_2, ...,i_n$ as input from user's intention (UI)
2) Let r as the list result of <intention, role> that users have
3) Let *idt* as the subset of Intention-Demand Tree that shows the relationship of intentions and demands which the users have
4) Let I_p as the Intention of the specific purpose of IDT
5) for each p_i in UI where i=1,2,..., n do
6) if (PT.hasNode(p_i) and K(p_i)∈Kp)
7) r.push(p_i,k_p(p_i)); // Push node p to K tree
8) for each a_i in r where i=1,2,3...,n-1do
9) for each b_j in r where j=1,2,3...,n do
10) if ((a_i not equals b_j)and(diff(a_i, b_j) <e)){
11) if(a_i.isParent(bj)) // confirm $a_i$node is Parent of bj
12) idt.push($a_i \rightarrow b_j$);
13) else
14) idt.push($b_j \rightarrow a_i$);}
15) inputidt into Specific Permission List;
16) Let spm_1, spm_2,...,spm_n as elements of List<Specific Permission>
17) for each spm_i in SPM where i=1,2,...,ndo
18) if(spm_i∈Role Permissions and (r isRoleOf UIc)){
19) for each $p_j$in SPwhere j=1,2,...,ndo
20) if ($p_j \rightarrow$SPMi){
21) SPM r.push(spm_i); }
22) }
23) return SPMu

The proposed model is tested in environments of various cloud service providers, being public, private and hybrid environments. This has shown justifying results over the common misbelieves that private cloud are enforcing more securing features to protect the information [18] and public clouds are not. Irrespective of the nature of cloud service providers, the security mechanisms implemented is the significant feature to rely on. Thus, this proposal may be implemented in any form of environment. It is already stated that this proposal does not have a huge impact on the background design and operations. In our next work, we plan to introduce a key security approach to enhance the sturdiness of this model. This is to make public cloud service providers more approachable for healthcare industries. Authentication, Authorization, and accounting are important processes that make a service more reliable. Right people should be provided with right access and rights to malicious users should be limited or zero at all. Claiming users and the provided information to new requests is a challenge to be addressed in near future. When such a platform is proposed, the legal issues between different nations which are opting for data sharing has to be discussed. The algorithm will attempt to retrieve a permission list which is assigned not based on the role defined in the system but on the basis of demands raised by the user. The details of medical knowledge, concepts and their relationships are considered so that the right user is not rejected of what they deserve. Permissions will be closely associated with their intentions of entering the system and list of patient files they wish to access. When the intention and demands form a relationship, a new permission list is provided by the system. Final output will be provided to users if they satisfy the initial criteria, by mentioning the right intention. For example, if a doctor intends to view files of patients who are admitted in another sector of medicine, the new demand rises. This condition when reached the narrowing levels of intention will cross out his new request or demand an authorization from existing doctors who are in charge [19]. Whereas, a nurse tries to take any decision-making attempts in the HIS, their demands will not be successfully retrieved by the system. Accounting will also be included to ensure that this approach is repeatedly monitoring. When an unbiased administrator is in charge of monitoring mechanisms, security of the system will be enhanced to a even better level [20].

IV RESULTS AND DISCUSSIONS

The model is investigated for its performance in a real time scenario where existing information systems were accessed. The medical records of cancer patients were utilized for investigating the functional capability of this approach. About 8500 records in a hospital with proper approvals were subjected to simulation. Cancers esophagus, kidney, stomach and blood are considered in this scenario. Total number of fields in each patient health record is 28, of which 12 were having personal and intimate details of them. Information about their real names, addresses, phone numbers, financial status and other transaction details are critical information which cannot be exposed to medically servicing persons. This system has a new intention and demand based permission assigning technique rather than a role based permission assignment technique.

The approach was tested in two bases for analyzing the strength of such an automated system in protecting patient information and relating the medical knowledge of participants with their roles.

A nurse is responsible for caring and providing medical attention to patients until they are discharges from the hospital. In order to facilitate proper care to a patient, all medically relevant information has to be made available to the nurse. Yet according to the policies of a hospital, certain permissions are provided and the system assigns a role based permission level to nurses when they access the system. These role based permissions are useless when the nurses have a counter intention. Though the system assigns with a patient based access rights, when a nurse intends to retrieve information beyond their limits, role based assignments do not possess any protection. But the figure 3 distinguishes how the role based and intention based models differ and level of security they provide over exposure of sensitive information. The role of nurse with a crooked intention will be eliminated by implementing the Intention-Demand Tree based permission assignments. In normal access control methods, the nurse may be able to track down all information about a patient with all necessary access rights. Their intention is undoubted by the system, since they are entitled with such rights. But in our proposed approach, the system verifies the demand by a request initiator though they are registered users in the system. When their intention and demands are justified, the requested permission will be granted. Similarly, if the justification is missing, respective officials are informed about their activity for necessary counter measures. Figure 3 denotes the number of iterations in vertical axis and security over patient information in the horizontal axis. This states that the levels mentioned in Figure 2 has to be crossed to be able to retrieve information of a patient. When the information is intimate and sensitive, the system needs the user to clear more number of security levels to obtain the results. Otherwise the results will not exhibit any output. There is a considerable change in role based access rights and intention-demand tree based access rights. In role based, with just the suitable role, the patient information is cleared for exhibition to the wrong users. Another scenario of providing the patient records for research is stated in Intentions listed in previous sections. Provided with access controls of a doctor, in role based access control systems, a doctor will gain access to all medical records in the system. But the important question is whether a doctor demands personal information about a patient. Answer is NO. Concepts, Relationships and medical knowledge associated with a disease in forms of medical reports are required by a researching doctor. The Intention-Demand will identify the requirements of such participants and deliver them altered patient information after hiding sensitive information. Figure 4 compares the functionality of proposed approach with existing standards for controlling access. Open access control, Purpose based access control, knowledge-based access control mechanisms are compared with Intention – Demand Tree based access control strategy. The open access control method is the least secure option among the compared systems. A similar system is Purpose based method which intends to analyze the patients' purpose of visit into the hospital system but their demands are not cross verified as done in this approach. There is another challenge in it as the visitors may not express their original purpose and may provide with false responses. Questioning such visitors may also offend their feelings in some scenarios. With sufficient knowledge about the medical domain, the proposed method included all norms and considerations to protect the privacy of patients according to jurisdictions. This is an added advantage of the proposed technique over other standards. The access rights of users who have the common role may be the same. Yet their intentions may not be same. These criteria will provide limitations by new access control by evaluating the intention and demand.

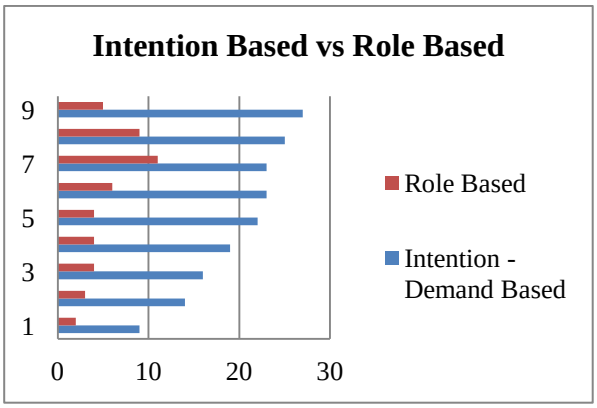

Figure 3. Intention Based vs Role Based

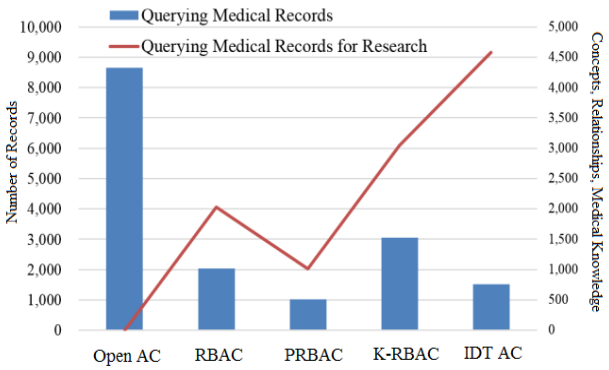

Figure 4. Protecting Privacy of Patients in Various Schemes vs Proposed Scheme

All access rights which are initially assigned according to the role of each participant will be changed when their intention and demand do not meet the prescribed medical knowledge and relative concepts. The same model may be efficient if implemented in a large medical institution where organization and maintenance need to be automated. It has to be understood that the input of this system is dynamic as well as assigning permissions to participants when a new need/demand arises. The model does not impose a big transformation in the original model for access controlling. A system with such specifications will be a better one in terms of permitting and preventing the right/wrong users.

V CONCLUSION

An access control scheme will be framed with the list of users and their mapped rights into contextual modules of information. This permits users with right roles but bad intentions to enter into a medical system for retrieving information which they are not supposed to access. Considering the sensitivity of information in a medical system, patients' private data and banking details, such access rights have to be revoked. This paper includes a technique which distinguished the access rights based upon the intention of a person who wants to participate in the medical system. Semantic mapping is done between the role, medical knowledge, concepts and demands imposed by the participant. With all available information found to be right, this approach will grant access to the user. Restrictions to data and scope of view are highly increased for a user with bad intentions. Privacy of patients is preserved by increasing the levels of security and reducing the accessibility rights when reaching the depth of information. From the obtained results after comparisons with existing methods, this approach is showing better protection to user information.

REFERENCES

1. K. Saleem, Z. Tan, andW. Buchanan, ``Security for cyber-physical systems in healthcare," in Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare, C. Thuemmler and C. Bai, Eds., Cham, Switzerland: Springer, 2017, pp. 233_251.
2. H. Journal, ``Summary of September 2017 healthcare data breaches," HIPAA J., Oct. 2017. [Online]. https://www.hipaajournal.com/september-2017-healthcare-data-breaches/
3. E. V. Eikey, A. R. Murphy, M. C. Reddy and H. Xu, "Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings," Int. J. Med. Informat., vol. 84, pp. 1065-1075, 2015.
4. R. Zhang, D. Chen, and X. Shang, "Privacy preserving for patients' information: a knowledge-constrained access control model for hospital information systems," In Proc. IEEE INDIN2016, Poitiers, France, 2016, pp. 921-926.
5. P. Hung, "Towards a privacy: access control model for e-healthcare service", *3rdConf. Privacy, Security and Trust*, New Brunswick, Canada, October 12-14, 2005.
6. Tiwari. M, Security policy speculation of user uploaded images on content sharing sites , IOP Conf. Series: Materials Science and Engineering 263 (2017) 042018 doi:10.1088/1757-899X/263/4/042019,pp-1-8.
7. S. Gritzalis, C. Lambrinoudakis, D. Lekkas and S. Deftereos, "Technical guidelines for enhancing privacy and data protection in modern electronic medical environments," *IEEE Trans. Information Technology in Biomed.*, vol. 9, no. 3, pp. 413-423, 2005.
8. L. Røstad and O. Nytrø, "Towards dynamic access control for healthcare information systems," *Studies in Health Technology & Informat.*, vol. 136, pp. 703-8, 2008.
9. L. Lee, Y. Chou, E. Huang and D. Liou, "Design of a personal health record and health knowledge sharing system using IHE-XDS and OWL," *J. Med. Syst.*, vol. 37, no. 2, pp. 1-12, 2013.
10. W. Hsu and J. Pan, "The secure authorization model for healthcare information system," *J. Med. Syst.*,vol. 37, pp. 1-5, 2013.
11. P. Sivakumar. Metrics Based Evaluation for Disease Affection in Distinct Cities. Research J. Pharm. and Tech. 2017; 10(8): 2487-2491.
12. C. L. Gordona and C. Weng, "Combining expert knowledge and knowledge automatically acquired from electronic data sources for continued ontology evaluation and improvement," *J. Biomed. Informat.*, vol. 57, Part C, pp. 42-52, 2015.
13. J. Lloret, S. Sendra, J. M. Jimenez, and L. Parra, ``Providing security and fault tolerance in P2P connections between clouds for mHealth services," Peer-to-Peer Netw. Appl., vol. 9, no. 5, pp. 876_893, 2016.
14. R. Kamatchi, K. Ambekar, and Y. Parikh, ``Security mapping of a usage based cloud system," Netw. Protocols Algorithms, vol. 8, no. 4,pp. 56_71, 2017.
15. Enterprise Cloud Computing: Transforming IT, Platform Comput. Inc, Markham, ON, Canada, Jul. 2009.
16. Bhanupriya Sharma, Augmenting SCA project management and automation Framework, IOP Conf. Series: Materials Science and Engineering 263 (2017) 042018 doi:10.1088/1757-899X/263/4/042018,pp-1-8
17. J. Brodkin, ``Gartner: Seven cloud-computing security risks," in Proc. Infoworld, 2008, pp. 1_3.
18. Cloud Computing Risk Assessment, Eur. Union Agency Netw. Inf. Secur., Heraklion, Greece, Nov. 2009.
19. A. Mehmood, H. Song, and J. Lloret, ``Multi-agent based framework for secure and reliable communication among open clouds," Netw. Protocols Algorithms, vol. 6, no. 4, pp. 60_76, 2014.
20. A. M. AlZadjali, A. H. Al-Badi, and S. Ali, ``An analysis of the security threats and vulnerabilities of cloud computing in oman," in Proc. Int. Conf. Intell. Netw. Collaborat. Syst., 2015, pp. 423_428.

AUTHORS PROFILE

Abirami. L, she received his UG and PG degree in Computer science discipline. She is doing his research in the area of machine learning in Health care domain. She published number of papers in referred impact factor journals. She registered her research work for the recognition of patent. abirami.2018@vitstudent.ac.in.

Karthikeyan J, He received Ph.D in VIT University, Vellore. UG and PG degree finished in computer science discipline. Presently, He is an Senior Assistant Professor in School of Information Technology and Engineering, VIT, Vellore. He has 11 years of experience in Teaching and Big data, Software testing and software Engineering field. His research interests include Software Testing, Software Engineering, Big data, Networking and Agile Testing. He is life time member of ISTE.karthikeyan.jk@vit.ac.in.