An Enhanced and Scrutinized, Secure Framework for Health Monitoring using IoT

R.Sujatha M.E, A.Ramanan, M.Logesh.

Abstract— ***Electronic health record (EHR) systems are used in healthcare industry to observe the progress of patients. With fast growth of the data, EHR data analysis has become a big data problem. Most EHRs are sparse and multi-dimensional datasets and mining them is a challenging task due to a number of reasons. In this project have used a nursing EHR system to build predictive models to determine what are all the factors impact death anxiety, a significant problem for the dying patients. Different existing modeling techniques have been used to develop coarse-grained as well as fine-grained models to predict patient outcomes. The coarse-grained models help in predicting the outcome at the end of each hospitalization, whereas fine-grained models help in predicting the outcome at the end of each shift, therefore providing a trajectory of predicted outcomes. Based on different modeling techniques, our results show significantly accurate predictions, due to relatively noise-free data. These models can help in determining effective treatments, lowering healthcare costs, and improving the quality of end-of- life (EOL) care.The DES based Public Key Cryptographic system of Identity Base Encryption is used for encryption of the Digital Signature. To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed. In this paper, in order to make e-health data's more secure we use multi party in cloud computing system. Where the health data is encrypted using attributes and key policy. And the user with a particular attribute and key policy alone will be able to decrypt the health data after it is verified by "key distribution centre" and the "secure data distributor". This technique can be used in medical field for secure storage of patient details and limiting to particular doctor access.***

Keywords: Electronic Health Record (EHR), Multi-dimensional Data set, Fine-Grained Models, Multi-Attribute based Encryption, Quantum Cryptography.

I. INTRODUCTION

Cloud Computing is the emerging technology, which is used to provide the different type of services to the user through the Internet [1]. Cloud system enables the data sharing mechanism which provide the variety of services to the user. According to the Information week survey all the organizations share 74% of their data with customers and 64% of their data to the supplier which is done with the help of the cloud [2]. So, the data sharing place an important role, higher priority and improves productivity in the cloud environment. The shared cloud services are easily accessible via the on-demand network access service and it is flexible which is available at lower cost [3]. During the data sharing the medical data or information sharing plays an essential role because the patient information's are easily accessible with minimum cost. Now-a-days the Personal Health Record (PHR) is one of the emerging technologies in the medical application which is used to create, manage and update the patient health information in an effective manner [4]. The PHR consist of several information about the particular patient like, identification sheet, problem or significant illness list, medical records, progress notes, consultation details, lab reports, immunization records, consent forms, imaging and x-ray reports and so on [5]. These information records are needed to be stored in the cloud for easy sharing and access mechanism which is used to control the activities of the patients. During the PHR information sharing the fine-grained access control, security, data confidentiality, authorization and authentication is crucial challenge while sharing the PHR records in the third party storage [6]. When the PHR data uploaded in the cloud environment the owner should lose their physical control also it is hacked by some intermediates and internal hackers. So, the security is a major challenge in the PHR data sharing in the cloud environment.

1.2. Problem Definition

We consider a PHR system where there exist multiple PHR owners and multiple PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. The users include readers and writers that may come from various aspects. There is also a central server belonging to the PHR service provider that stores all the owners' PHRs, where there may be a large number of owners. Users access the PHR documents through the server in order to read or write to someone's PHR. The PHR files can be organized by their categories in a hierarchical way.

II. REVIEW OF LITERATURE

We start with a review of related work on trusted VM launch, followed by storage protection in IaaS. Trusted Launch Sadiku et al. [1] proposed a "Trusted Cloud Compute Platform" (TCCP) to ensure VMs are running on a trusted hardware and software stack on a remote and initially untrusted host. To enable this, a trusted coordinator stores the list of attested hosts that run a "trusted virtual machine monitor" which can securely run the client‟s VM. Trusted hosts maintain in memory an individual trusted key

Revised Manuscript Received on April 12, 2019.

R.Sujatha M.E., (Ph.D.), Senior Assistant Professor, Department of Information Technology, M.Kumarasamy College of Engineering (Email: sujathar.it@mkce.ac.in)

A.Ramanan, Department of Information Technology, M.Kumarasamy College of Engineering (Email: ramananardr1998@gmail.com)

M.Logesh, Department of Information Technology, M.Kumarasamy College of Engineering (Email: logeshsharma10@gmail.com)

used for identification each time a client launches a VM. The paper presents a good initial set of ideas for trusted VM launch and migration, in particular the use of a trusted coordinator. A limitation of this solution is that the trusted coordinator maintains information about all hosts deployed on the IaaS platform, making it a valuable target to an adversary who attempts to expose the public IaaS provider to privacy attacks. A decentralized approach to integrity attestation is adopted by PrajaktaSolapurkar et al. [2] to address the limited transparency of IaaS platforms and scalability limits imposed by third party integrity attestation mechanisms. The authors describe a trusted architecture where tenants verify the integrity of IaaS hosts through a trusted cloud verifier proxy placed in the cloud provider domain. Tenants evaluate the cloud verifier integrity, which in turn attests the hosts. Once the VM image has been verified by the host and countersigned by the cloud verifier, the tenant can allow the launch. Our protocol maintains the VM launch traceability and transparency without relying on a proxy verifier residing in the IaaS. Furthermore, the TL protocol does not require additional tenant interaction to launch the VM on a trusted host, beyond the initial launch arguments. Platform attestation prior to VM launch is also applied in [7], which introduces two protocols – “TPM-based certification of a Remote Resource” (TCRR) and “Verify My VM”. With TCRR a tenant can verify the integrity of a remote host and establish a trusted channel for further communication. In “Verify My VM”, the hypervisor running on an attested host uses an emulated TPM to verify on-demand the integrity of running VMs.

Our approach is in many aspects similar to the one in [7] in particular with regard to host attestation prior to VM instance launch. We overcome this limitation and generalize the solution by adding a verification token, created by the tenant and injected on the file system of the VM instance only if it is launched on an attested cloud host. In [8], the authors described a protocol for trusted VM launch on public IaaS using trusted computing techniques. To ensure that the requested VM instance is launched on a host with attested integrity, the tenant encrypts the VM image (along with all injected data) with a symmetric key sealed to a particular configuration of the host reflected in the values of the platform configuration registers (PCR) of the TPM placed on the host.

The proposed solution is suitable in trusted VM launch scenarios for enterprise tenants as it requires that the VM image is pre-packaged and encrypted by the client prior to IaaS launch. However, similar to [7], this prevents tenants from using commodity VM images offered by the cloud provider to launch VM instances on trusted cloud hosts. Furthermore, we believe that reducing the number of steps required from the tenant can facilitate the adoption of the trusted IaaS model. We extend some of the ideas proposed in [8], address the above limitations – such as additional actions required from tenants – and also address the requirements towards the launched VM instance and required changes to cloud platforms.

III. DATA SECURITY MODEL

In this section, in particular data security in cloud computing is examined. In today's world the most important security problem in the use of cloud computing at all levels is data security problem. In data security, confidentiality, integrity and availability of data in cloud computing are referred.

A. Data Confidentiality in Cloud

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Data confidentiality is one of the most difficult things to guarantee in a cloud computing environment. In Cloud computing environment, two categories of confidentiality exists: confidentiality in private cloud and confidentiality in public cloud. Because the confidentiality in private cloud is like a simple private network, we go through the public ones. In public cloud there are some potential concerns about confidentiality. First, are there any access controls to protect the data? Access control consists of authentication and authorization. Today’s the ways providers ensure that users are adequately authenticated when using browsers to access services in the cloud are limit.

They must use strong ways in addition to username and password checking. Some new ways are 2 or 3 factor authentication or web proxy logon [6] and using Security Assertion Markup Language (SAML) standard. With SAML, each organization manages its own users and through trust relationships share authentication between sites. SAML is an elegant solution for scalable authentication. Authentication for the cloud will rely on SAML and provide the dual benefit of reducing the number of passwords that users must remember as well as improve user experience through Single Sign On (SSO).

Second, are there any data encryption methods while data is transiting between end-user’s client and the cloud’s server? Data encryption is useful for kind of data that is stored on cloud servers and the users don’t need to index or search them. About data-at-rest in IaaS encryption is a good idea, but encrypting data-at-rest in that a PaaS and SaaS cloud-based application is using as a compensating control is not feasible [7]. There are some works which allows data to be processed without being decrypted such as homomorphic encryption [8] and predicate encryption [9] that are underway.

B. Data Integrity in Cloud

Integrity is the assurance that the information is authentic and complete. The integrity of data is not only whether the data is correct, but whether it can be trusted and relied upon. Since 1980’s we use “ACID” (atomicity, consistency, isolation, and durability) principles in our database management systems to ensure about data integrity but cloud computing is new enough that not all service providers have satisfactorily incorporated these data integrity principles in their solutions. Moreover, customers sometimes use such a variety of service providers that no single one of them takes responsibility for ensuring data

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

integrity at the level of data entry and transaction management. There are some new standards that are related to cloud data management and over the time they are developing. Cloud Service providers must use and develop such standard to ensure their users about the integrity of cloud data. Internet is the media that are used in cloud computing and often the entry of it, is web applications. Some of the standards that are developing in today's cloud world are Data Integrity Field (DIF), SNIA Cloud Data Management Interface (CDMI), and XML-based solutions.

C. Data Availability in Cloud

Availability is the assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. The most problematic issue in security of cloud computing is availability. Many of cloud service providers experienced downtime. There are some ways to provide data availability for customers for example some cloud service providers do back up customer data, or a better way is a caching proxy server that can reply to service requests without contacting the specified server, by retrieving content saved from a previous request, made by the same client or even other clients.

Another way to have availability is switchover from the online-server to the hot-standby server. These range from storage mirroring across multiple servers which ensures that a server failure never results in data loss, to the ability to recover from a failure of the cloud controller, to high-availability features built into the catalog appliances. The ability to easily run two identical instances of the application on the same cloud, or in different data centers, provide the ultimate approach to high availability.

IV. PROPOSED APPROACH

It focuses on the analysis of nursing care data within EHR systems, which is an important but often ignored component of the EHR. Nurses are the front-line providers of care so the data they enter into HER systems is extremely imperative to the improvement of patients' care. Mining the nursing data can potentially help guide more effective treatment of patients and thus to help reduce costs and produce better patient outcomes.

The Original Data is encrypted with the key and a cipher text is generated. Here the DES technique is used. The Digital signature of the sender is encrypted with the help of key (Attributes) and an encrypted Digital signature is generated. ABE technique is used. The Encrypted Digital Signature is deciphered using the key and the original message is retrieved. Only if the Digital Signature matches, the cipher text can be deciphered.However, in MA-ABE the access policies are enforced in users' secret keys, and the policies are fixed once the keys are distributed which is not convenient for owners to specify their own policies. By our design, we show that by agreeing upon the formats of the key-policies and specifying which attributes are required in the cipher text, the supported policy expressions enjoy some degree of flexibility from the encrypt or's point of view. However, if any of the authorities (hospitals) misbehave, it can decrypt all the data of owners who allow access to users in that hospital. This is clearly against the patient-centric privacy concept. In addition, this method is not efficient since the policies for the three hospitals are duplicated, which makes the cipher text long.

V. IMPLEMENTATION &THEORETICAL RESULT

The health monitoring gives precise information on the corporal effort that is taking place at each time. A simple analysis method consists in checking that the health rate is within a safe range. In this case the organization knows that all rates for each person should be between a lower and an upper threshold. Therefore, if one of the health rates exceed the upper threshold or its value is lower than the lower threshold, the system alerts the medical staff. However, other papers on irregularity detection from data are using presumption methods based on dynamic programming techniques and other mathematical operation in order to detect deeper heart anomalies that may cause injuries, even when the health rate is within safe range. These studies allow real-time monitor of the effort rate made by muscles and the measurement of the neuromuscular function. The obtain data include a number of parameters of physical activity such as average power, normalized power, speed, force, and acceleration. The aim of this proposal is to optimize the use of biomedical sensors and computing resources for being able to provide advanced application to the user. The main contribution of this paper is the design of a dispersed computational framework to use the available computing capabilities of the smart devices for sharing the processing of highly developed health monitoring applications. The target audience of this work covers an interdisciplinary set of specialized including computer scientists, doctors, coaches, directors of sports middle, among others.

VI. CONCLUSION

As computing takes a step forward to cloud computing, we must pay attention to security issues of it. Because of security concerns, cloud computing is not concerned with some users. As a virtual environment cloud computing has its special security threats and these threats are completely different from threats in physical systems. In this paper, security concerns about data security in cloud computing is examined and a new model suggested for this environments. In this model security concerns and their solutions are categorized in three layers of security services to secure accessing to data resources in cloud worlds. Although you may be transferring some of the operational responsibilities to the provider, the level of responsibilities will vary and will depend on a variety of factors, including the service delivery model (SPI), provider service-level agreement (SLA), and provider-specific capabilities to support the extension of your internal security management processes and tools. In this model, the relationship between end users and cloud service providers is showed and according to their responsibilities in providing data security in cloud

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

environment, a new solution for it is proposed. Because in information security, most foundations can be built upon confidentiality, integrity, and availability, and CIA is a widely used benchmark for evaluation of information systems security, this model can be a good idea in cloud world that is a new world.

Our future work will comprise how to secure the access of the data and will develop a mobile submission that allows access of the data on handheld devices. Implementing adetection engine over IoT network is resource overwhelming asthey are based on AI algorithms. Hence, novel lightweightsolutions for detecting Denial-of-Service attacks are required. Apart fromnovel insubstantial solutions, emerging paradigm of Software Defined Network (SDN)enables monitor of network state from a central pointcalled controller. By supervise flows at the controller; it ispossible to implement algorithms to detect DDoS attacksand malicious behavior such as insider attack.

REFERENCES

1. Sadiku, Musa, Momoh, “Cloud Computing: Opportunities and Challenges”, IEEEPotentials, Volume 33, Issue 1, 2014.
2. PrajaktaSolapurkar, GirishPotdar, “A Survey on Secure Data Sharing and CollaborationApproaches in Cloud Computing”, International Journal of Science and Research, 2012.
3. Harish Reddy, Venkat Reddy, JeevanaJyothi, “Security Issues in Cloud Computing Services”, International Journal of Advanced Research inComputer Science and Software Engineering”, Volume 3, Issue 6, June 2013.
4. Eapen B.R., Chapman B. Mobile Access to Clinical Connect: A User Feedback Survey on Usability, Productivity, and Quality. JMIR mHealth and uHealth 2015; 3(2):e35.
5. Charlotte Seckman, “Electronic Health Records andApplications for Managing Patient Care” Information Systems in Healthcare Delivery in Elsevier, 2013.
6. Ming Li, Shucheng Yu, Yao Zheng, KuiRen,Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption”, IEEE Transactions On Parallel And Distributed Systems, 2012.
7. Xiaolin Si, PengpianWang; Liwu Zhang, “KP-ABE Based Verifiable Cloud Access Control Scheme”, IEEE International Conference onTrust, Security and Privacy in Computing and Communications (TrustCom), 2013.
8. LonghuiZu, ZhenhuaLiu; Juanjuan Li, “New Cipher text-Policy Attribute-Based Encryption with Efficient Revocation”, IEEE International Conference on Computer and Information Technology (CIT), 2014.
9. S.Palanivel Rajan, T.Dinesh, “Statistical Investigation of EEG Based Abnormal Fatigue Detection Using LabVIEW", International Journal of Applied Engineering Research, ISSN: 0973-4562, Vol. 10, Issue 43, pp.30426-30431, (Impact Factor – 0.127), 2015.
10. Perumal, Rajasekaran, Duraiyarasan, “An efficient hierarchical attribute set based encryption scheme with revocation for outsourcing personal health records in cloud computing”, Advanced International Conference on Computing and Communication Systems (ICACCS), 2013.
11. Sharma, Balasubramanian, “A biometric based authentication and encryption Framework for Sensor Health Data in Cloud”, International Conference on Information Technology and Multimedia (ICIMU), 2014.
12. S.Vijayprasath, S.Palanivel Rajan, “Performance Investigation of an Implicit Instrumentation Tool for Deadened Patients Using Common Eye Developments as a Paradigm”, International Journal of Applied Engineering Research, ISSN No.: 0973-4562, Vol. 10, Issue No.1, pp. 925-929, 2015.
13. S.Palanivel Rajan, V.Kavitha, "Diagnosis of Cardiovascular Diseases using Retinal Images through Vessel Segmentation Graph", Current Medical Imaging Reviews (Bentham Science Publisher), Online ISSN No.: 1875-6603, Print ISSN No.: 1573-4056, Vol. No.: 13, Issue : 4, pp. 454-459, (Impact Factor–0.613), 2017.