International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 4, Issue 10
October 2016.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

Received on: 01.10.2016 Published on: 28.10.2016 Pages : 47-52

Monitoring real time data and secure retrieval for Telemedicine systems

[1] K.Arun Prasad [2]K.Pushpavalli,[3] S.Syed Basha
Department of Information Technology, Agni College Of Technology, Chennai, India

Abstract— Most of the victims undertaken vital surgeries require regular monitoring of their health parameters. There they are vault to physical boundaries which restrict their movement. We use a belt which is tied to the wrist and continuously monitors the temperature and heart rate of the patient. This data is sent to the hospital server and is take care by the physician. They are alerted when there is a drastic change in the observed parameters. Based on the BSID technique, any sort of intrusion is identified by differentiating the observed readings with the state table which contains the standard values for the parameters. The health records of the patient are stored in a centralized cloud and can be fetched from anywhere in the globe. Distributed cloud computing allows exclusive treatment of the persons during medical consultation by sharing patients health records among different hospitals. Here, the secrecy of the data and patients' identity privacy are preserved by applying a novel AAPM. Patients can authorize doctors by setting up an access tree. By using PSMPA technique we can establish three security levels. The doctor who is responsible to care for the patient has full access to his records. The referred doctors cannot have certain privileged regarding modification of the data. Any other person is considered to be unauthorized.

Introduction

Health is one of the increasing concern among people. Nothing else matters if one gets sick. This resulted in people spending more money for caring their health. But, we find that it is useless to get medical attention when the condition becomes helpless, that is the disease is identified in advanced stages. A great percentage of patients can be cured, if actions are taken on time. Moreover, the access to the medical equipment is not easy or affordable. Among others, the body temperature and the heart rate are the important ones in human health. The measure of body temperature and heart rate has no harm on health of the patients. It is the general behavior of the body to keep its body temperature within a narrow, safe range although there exists large variations in temperature outside the body. The typical body temperature of human is expected to be around 37.0 °C ± 0.4°C (98.6 ° F ± 0.7°F)

Heart rate drastically changes between individuals based on age, fitness and genetics. Normal heart beat of a person in rest is about 70 bpm for men and 75 bpm for women. The heart and body temperature values are monitored frequently for normal functioning of body and to maintain health.

The received temperature and heart beat values known as the real-time values is checked for intrusion. Any change in the recorded parameters may result in more serious issues, as it relates to the patients' health condition. By using behavior-rule specification based intrusion detection (BSID) technique, the changes made in data(intrusion) is found accurately and actions are taken. Storage of all these datas are done in a cloud provided by amazon. It enhances the retrieval more efficient by allowing access from all over the globe.

Patient Monitoring System Background

Monitoring patients' health status anytime and anywhere without limiting the patients' movement by tying down through cables to the monitoring equipment is an important application. Through the reduction in size of

sensors and the use of wireless interface to transmit the data recorded by the sensors, healthcare monitoring can be extended beyond hospital boundaries. We consider a patient monitoring system (PMS) with sensors to monitor the heart rate and the temperature of the patient through the use of wireless communication. The physicians can be able to monitor the patient's advancement or deterioration in health without having to spend on the cost of hospitalization. When an alarm condition occurs in a patient, that is the recorded value is above or below the marked threshold value, the physician will be notified by the admin to take appropriate action.

For streaming live health condition, we have developed a system that not only measures heart rate and temperature accurately but also transmits data simultaneously to the web server. We are concerned about intrusion of the observed readings from the PMS where patients' healthcare personnel can depend with high confidence. The detection mechanism we use is based on behavior rule specification. Behavior rule for a device is specified during the design phase of PMS. We design a state table which specifies expected normal behaviors for each device and can detect deviation. Our intrusion detection protocol takes as input, the set of behavior rules for the device and detects if the device behavior deviates from the expected behavior by comparing with the state table.

Once the health information that is, the real-time data is identified to be free from intrusion, they are stored in a central cloud. Other patient related data such as his health reports, scans, and the medicines prescribed can be recorded securely. This is useful when a patient wishes to have a second opinion about his health condition , he can access all his records from the previous hospital and need not perform all the tests once again. It saves money as well as time.

state table creation

State table contains the standard values of the normal heart beat and temperature. It is stored in the cloud. Once the real-time data reaches the cloud, it is checked against the state table values for any intrusion. As the health parameters are vital for ones healthy existence, any change in the stored values greatly impact the medication of the patient. As telemedicine system does not involve direct interaction between patient and physician, any change in the recorded values have greater impact in change of medication.

Age	18-25	26-35	36-45	46-55	56-65	65+
Athlete	49-55	49-54	50-56	50-57	51-56	50-55
Excellent	56-61	55-61	57-62	58-63	57-61	56-61
Good	62-65	62-65	63-66	64-67	62-67	62-65
Above Average	66-69	66-70	67-70	68-71	68-71	66-69
Average	70-73	71-74	71-75	72-76	72-75	70-73
Below Average	74-81	75-81	76-82	77-83	76-81	74-79
Poor	82+	82+	83+	84+	82+	80+

Fig1: Sample State Table

Behavior rule for a device is specified during the design phase of PMS. We design a state table which specifies expected normal behaviors for each device and can detect deviation. Our intrusion detection protocol takes as input, the set of behavior rules for the device and detects if the device behavior deviates from the expected behavior by comparing with the state table.

Representational State Transfer

REST stands for Representational State Transfer. It relies on a stateless, client-server communication protocol which can easily be cached and in virtually all cases, the HTTP protocol is used. REST is an architecture for designing applications in networks. Web service APIs that adhere to the REST architectural constraints are called RESTful APIs. REST uses Async task to transfer data to the server. It is primarily used to build web services that are lightweight, maintainable, and scalable. REST is used to minimize the coupling between client and server components in a distributed application. They are used in a special case where the server is going to be used by many different clients which cannot be controlled. It may also be the case if you want to update the server regularly without updating the software of the . Using this service, the real-time data reaches the cloud server efficiently when there is heavy data traffic.

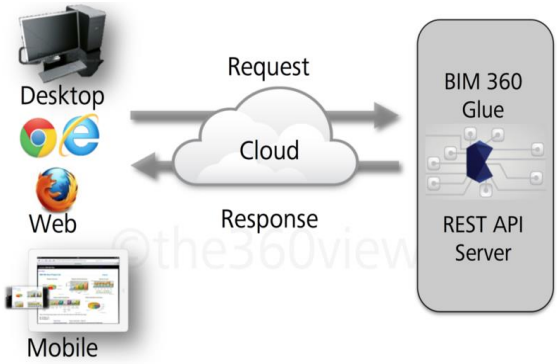

fig2: rest architecture

Intrusion Detection Mechanism

The detection mechanism used for intrusion here is behavior-rule based IDS. Intrusion detection techniques in general can be classified into four types: signature, anomaly,
trust, and specification-based techniques. We consider specification rather than signature-based detection to deal with unknown pattern of the attacker. We consider the technique of specification rather than anomaly based techniques to avoid using resource- constrained sensors or actuators in an PMS for profiling anomaly patterns (e.g., through learning) and to avoid high false positives. We consider the technique specification replacing the technique of trust to avoid delay due to trust aggregation and propagation which results in quick reactions to malicious behaviors in a system where safety is the key as in PMS. To accommodate resource-constrained sensors and actuators in an PMS, we propose behavior-rule specification based intrusion detection (BSID) which uses the notion of behavior rules which specifies the behaviors that are acceptable for medical devices in an PMS. Rule-based intrusion Detection thus far has been applied only in the field of communication networks that have no concern of physical environments and the closed-loop control structure as in the PMS.

Techniques Used

To share medical information among healthcare providers to enable effective treatment of patient, distributed cloud is used. Here the main issue faced is preserving the information from eavesdroppers. The secrecy of the data and the identity of the patient has to be well preserved. The access control authentication scheme we use here is authorized accessible privacy model (AAPM). Patients can authorize doctors by setting an access tree having suitable attributes. To implement three levels of security, a new technique of attribute-based allocated signature of the verifier, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) is introduced. Each of the levels can access the records based on the attributes provided to them. They can respectively decode or retrieve the patients' health information and/or verify patients' identities by satisfying the access tree with their own attribute sets.

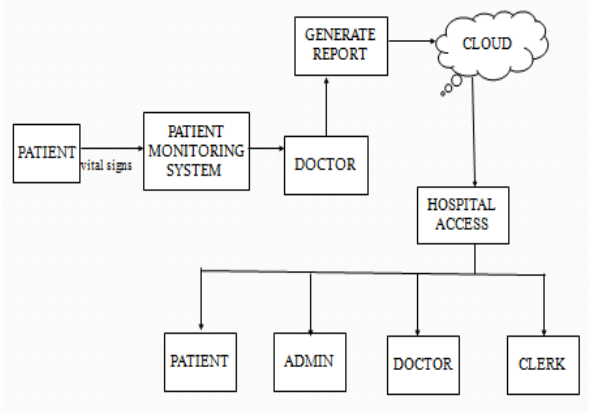

Fig3: OVERALL ARCHITECTURE

Distributed Cloud

Cloud storage becomes useful in the facet that the data is available centrally and can be retrieved from elsewhere in the world. As the health related data can be stored, the need for carrying hard copy of the reports can be completely avoided and can be retrieved whenever and wherever required. Another advantage of storing

the health information in cloud is that, in a life threatening situation of a patient, he may go for consulting more than one hospital needing a solution. As to the security facet, one of the main issues is access control of patients' personal medical information, where only the authorized physicians or institutions that can recover the patients' personal health records during the sharing of data in the distributed m-healthcare cloud computing system. In practice, most patients are worried about the confidentiality of their personal medical information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared.

Cloud Environment

Administrator

The cloud storage enables the doctors and the patients to simultaneously access the health information. An administrator called as admin gives access rights to doctors. He is the one to add the doctors to the cloud environment. The clerk in the hospital gives the access rights to the patients as they are admitted.

Whenever a patient is admitted, his personal information along with the previous medical history is also stored in the cloud. Each patient as well as the doctor is given a login id and password for authentication. There exists the admin who is the central controller of the hospital. He has access to all of the records.

Audit Logs

There is an option called *log* which tracks the activity of cloud usage. Log audit specifies the exact date and time at which the particular doctor or patient has accessed the records with an indication of what action is made. It is helpful in a way to search health records within a particular period. Audit logs contains entry for every action made it is capable of retrieving records based on 1)patient id 2)date wise patient admission across a city 3) a particular patient in a particular date 4)disease wise admission in a certain period 5) based on the doctors.

Medical transcription

This is nothing but the prescription that suggests the patient, a certain dosage of drugs for a certain time period. In this scenario, an option is available for the doctors to pull the records of his patient which includes the real-time data values of live heart beat and temperature. Based on the deviation in his health parameters, the dosage of medicines even the course of medication can be changed. All this can be done remotely by the doctor. There is no necessity for the direct interaction between the doctor and patient. As with telemedicine systems, this can be achieved by storing the health records centrally in cloud. The specialists could not be available at all times. This feature provides an easy way to overcome the problem.

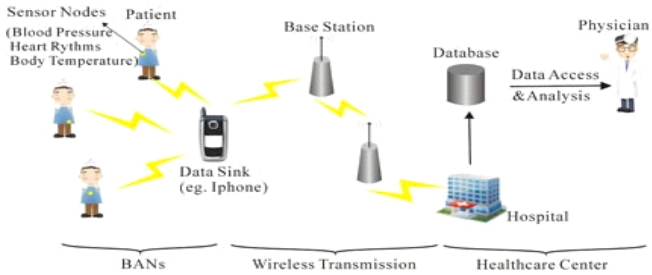

Fig4: Architecture of e-health system

Data confidentiality and Identiy privacy

Distributed cloud computing bring about a series of challenges, especially how to ensure the security and privacy of the patients' medical information from numerous attacks in the wireless communication channel such as eavesdropping and tampering. As to the security facet, one of the main issues is access control of patients' personal health information, as it is only the designated physicians or institutions that can recover the patients' personal health information during the time of sharing data in the distributed healthcare cloud computing scenario. In practice, most patients are concerned about the secrecy of their health information since it is likely to make them in issues of unauthorized collection and disclosure. Therefore, in distributed healthcare cloud computing techniques, what part of the patients' health information should be used by others and which

physicians their personal health records should be shared with have become two growing problems needing urgent solutions.

Notification

Admin can notify doctors in case of any emergency. A notification message specifying the condition of the patient can also be added. Once the respective doctor logs in, a notification message pops up in his screen. The status of the action is also notified. Once the doctor acknowledge the urgent message, the flag is set as action done else action is pending. The status flag is indicated by colors – red for pending action and green for action made. For example , doctor Ganesh ganesh@gmail.com is notified with the urgent message patient critical. Once he logs with his id, a notification pops up in his window and he could take quick action.

Displaying graphs and reports

The real time data of the patient that is the heart rate and temperature values will be consolidated in a graphical representation showing their performance. Also we can upload the scans and x-ray report in the cloud which can be accessed whenever and wherever needed. The doctor can have access to these information and suggest for suitable changes in the medication course. A detailed report of the ailment suffered, the side effects and the treatment course are all recorded safely by the concerned doctor. The patient has access to his records whenever needed. He needs to remember the login id and password for authentication.

Sharing patient records

In health care social networks, the personal health information is always shared among the persons located in respective social communities suffering from the same disease for mutual support and across distributed health care providers for medical consultation. There is an exclusion option of sharing patient records among other doctors. This will be useful in research purpose as well as knowing the growth rate of a particular disease. Once the patient has been taken care of, the proceedings done in the name of treatment are recorded digitally. The total medical history of the patient is made available for future reference. They also remain as a case study for research purpose.

Specifications

We use Bluetooth to transfer real time data to the hospital server. This data reaches the cloud through the internet. REST(REpresentational State Transfer)service processes the request and uses async task. The cloud server we use is provided by the amazon web services. We use MongoDB to store the health information. MongoDB is a cross platform and also the database is strictly adhered to documents. It is a nosql database. The processing is done through nodejs framework.

Conclusion

we have shown a design of a newly developed remote heart rate and body temperature monitoring device. The final result of our methodology is to monitor the health condition remotely and to measure the parameters with a flexible architecture that can be readily adopted in several different fields of application. The system has been tested and verified for the heart rate and body temperature. A novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme establishing three levels of security and privacy requirement in the distributed healthcare cloud computing system are suggested, followed by the usual security proof and efficiency evaluations which illustrate our PSMPA can avoid different kinds of malicious attacks and far outperforms previous schemes in terms of storage, computation and communication overhead.

References

[1] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, “Security challenges in next generation cyber physical systems,” Beyond SCADA: Netw. Embedded Control for Cyber Phys. Syst., Pittsburgh, PA, USA, Nov. 2006.

[2]A.C.ardenas,S.Amin,B.Sinopoli,A.Giani,A.Perrig,andS.Sastry, “Challenges for securing cyber physical systems,” in Proc. 1st WorkshopCyber-Phys.Syst.SecurityDHS,2009,pp.1–4.

[3]I. R. Chen, A. P. Speer, and M. Eltoweissy, “Adaptive fault tolerant QOS control algorithms for maximizing system lifetime of query-based wireless sensor networks,” IEEE Trans. Dependable Secure Comput., vol. 8, no. 2, pp. 161–176, Mar./Apr. 2011.

[4]J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Rel., vol. 59, no. 1, pp. 231–241, Mar. 2010.
[5]A. daSilva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. 1st ACM Int. Workshop Quality Service Security Wireless Mobile Netw., 2005, pp. 16–23.
[6]K. Ioannis, T. Dimitriou, and F. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 13th Eur. Wireless Conf., 2007, pp. 1–7.
[7]I. Lee and O. Sokolsky, "Medical cyber physical systems," in Proc. 47th ACM Des. Autom. Conf., 2010, pp. 743–748.
[8] Y. Li and I. R. Chen, "Design and performance analysis of mobility management schemes based on pointer forwarding for wireless mesh networks," IEEE Trans. Mobile Comput., vol. 10, no. 3, pp. 349–361, Mar. 2011.
[9]R. Mitchell and I. R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," IEEE Trans. Rel., vol. 62, no. 1, pp. 199–210, Mar. 2013.
[10] K. Park, Y. Lin, V. Metsis, Z. Le, and F. Makedon, "Abnormal human behavioral pattern detection in assisted living environments," in Proc. 3rd ACM Int. Conf. Pervasive Technol. Related Assist. Environ., 2010, pp. 9:1–9:8.
[11]P. Porras and P. Neumann, "EMERALD: Event monitoring enabling responses to anomalous live disturbances," in Proc. 20th Nat. Inf. Syst. Security Conf., 1997, pp. 353–365.
[12]K. Venkatasubramanian and S. K. S. Gupta, "Security solutions for pervasive healthcare," Security in Distributed, Grid, Mobile, and Pervasive Computing, New York, NY, USA: Auerbach, 2007.
[13]L. Gatzoulis and I. Iakovidis, "Wearable and portable E-health systems," IEEE Eng. Med. Biol. Mag., vol. 26, no. 5, pp. 51–56, Sep.-Oct. 2007
[14]I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare records in europe,"Int.J.Med.Inf.,vol.52,no.1,pp.105–115,1998.
[15]M. D. N. Huda, N. Sonehara, and S. Yamada, "A privacy management architecture for patient-controlled personal health record system," J. Eng. Sci. Technol., vol. 4, no. 2, pp. 154–170, 2009.
[16]D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner, and J. Thierry, "Anonymity and application privacy in context of mobile computing in eHealth," in Mobile Response, New York, NY, USA: Springer, 2009 pp. 148–157.