ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

A New Technique for ECG Telemedicine Data Security and Privacy Using Digital Signature and XML Database

Md. MominReja[1], Sonia Corraya[2], UmmeSaymaBusra[3]

Department of CSE, Jahangir Nagar University, Savar, Dhaka[1]

Faculty, Department of CSE, BRAC University, Dhaka[2]

Department of CSE, Jahangir Nagar University, Savar, Dhaka[3]

Abstract: Security of telemedicine information is an uncompromising issue as this is a matter of life risk. Outdated security standards affect the overall efficiency of telemedicine system. Recent studies on latest telemedicine security research shows that only 61% proposed a solution and 20% of these tested the security solutions that they proposed. In this paper a new methodology is proposed for ECG telemedicine system using advance technology. In this new technique ECG data is digitally signed and stored in Sedna XML database before sending to doctor.Medical care is only provided by the physician only after successful data retrieval with valid authentication. Subsequently the proposed technique is tested with 30 sample ECG medical records and evaluated by comparing the results from both traditional and proposed new ECG telemedicine system with XML Digital Signature. Initial finding shows promising result; the new security scheme reduced the security risk to 3.33% only from 20%

Keywords: XML; Digital Signature; Sedna; Telemedicine; ECG; Pushmodel; XCA

I. INTRODUCTION

Security and protection of telemedicine data determines the overall success of telemedicine implementations. Accuracy of tele-healthcare depends on the security mechanism while transferring tele data over internet with the use of information technology and telecommunication. Authentication, integrity and confidentiality ofpatient's data are often pointed out as key factors to be considered in medical information system [2].Recent studies on latest telemedicine security research shows that only 61% proposed a solution and 20% of these tested the security solutions that they proposed [12].

In a telemedicine system the patient should be able to trust the system.Inaccurate telemedicine data as well as its resulting wrong interpretation increase the risk at patient side. Thus reliability is an important concern. Thus telemedicine systems should also be evaluated for perceptions of both patients and caregivers since they may be perceived as intrusive and ineffective [3],[4]. While several security challenges in telemedicine are common to all information-technology-based systems, there are unique questions that need further attention. Reliability and availability is a key issue, as many of these systems might be critical life-supporting systems. It is also important to maintain the usability of these systems without compromising the security [5].

Hence our main objective is to use cryptography technology for telemedicine data transformation through secured or unsecured channel. To make the data more secure 'Digital Signature' and XML database (Sedna) is used in our new and advanced telemedicine system: ECG. The teledata have to be hashed first. The signer will encrypt the XML data with his private key including a public key. The receiver must have to get the public key to decrypt the data. To ensure that the data is from the right party, the Certifying Authority will also sign the data with his private key and a public key. On the receiver end if the receiver find that the data is authorized he will be confirmed that it's a signed data.

The remainder of the paper is organized as follows: section 2provides the rational of the study. The research Methodologyis described in section 3. Description of system structure isdiscussed in section 4. Section 5 provides the systemrequirement. ECG System with XML Digital Signature system design are discussed insection 6. Systems outcomes are described in section 7. System outcome and performance analysis are given in section 7 and section 8 respectively. Limitations of the system are explained in section 9 and finally the conclusion is drawn in section 10.

II. RATIONAL OF THE STUDY

Normally, communication is represented as a flow ofinformation from a source to a destination. However, withsecurity threats like interrupting, jamming, in personification, flooding, modification, virus [8]; it can take a new modified form.

Since telemedicine involves the use of internet toconnect patient and the health care givers, it makes itvulnerable to attacks and most of the network attacks arepossible on telemedicine data. The attacks can be grouped into two broad categories of active and passive attacks. Active

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

attacks involve attacker to engage inmodification, interruption or fabrication of patient imagesand information such as replay orretransmission toproduce an unauthorized effect, modification of messageas well as Masquerade; pretends to be some other entity and denial of service Passive attacks are mainly where attacker merely eavesdrops and monitors a system performing its tasks and collecting information.

This includes interception of information, though not alteration or addition of information. Traffic analysis of information involves observing message patterns service to valid users and release of message content which may be carrying sensitive or confidential data read by an attacker. [2].

One of the oldest and common tools available forms of data protection is by means of encryption. Encryption protects contents particularly during transmission of data from sender to receiver. However, once it reaches a recipient and decrypted, the protection ends and the data can be copied and redistributed without further complications [6],[7]. This is because the object loses its protection once it is decrypted. Consequently, mishandling of sensitive information cannot be prevented effectively by this traditional means. Study in [1],[8] confirms that using encryption is insufficient to protect the confidentiality of patient telemetry.

III. METHODOLOGY

It was an experimental research in design. At first we tested 30sample patient telemedicine data and test the output result in both traditional and out proposed new telemedicine system. The observed result of both output by expert physicians has lead us for the unmet need for security and privacy of ECG services by using Tele-medicine technology. We have conducted experiment of our model in laboratory environment only. Fig. 1 shows the traditional ECG System model.

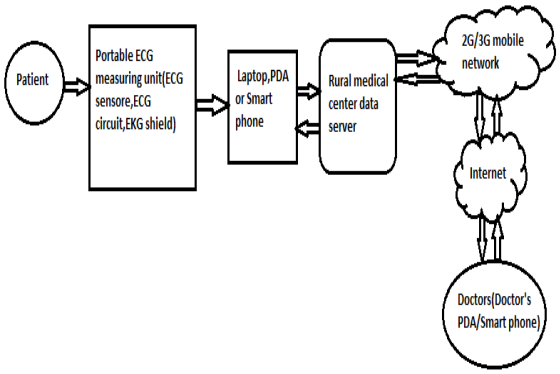

Fig.1. Traditional ECG System model without any data security mechanism[9]

IV. SYSTEM STRUCTURE

In this research, we attempted to design a secure telemedicine system, especially for tele-diagnosis, using XML Digital signature, medical toolkit and android/Java technology[9]. For this proposed system; here we have to use a medical toolkit, which is capable of measuring daily health conditions of electrocardiogram (ECG), and this digital signal is transferred to a receiving device (ECG Circuit) for signal processing and we use EKG shield for converting them as usable for 3G/2G network[9]. Then this digital signal or data will be used for laptop/ Android Phone by parsing (SAX parser) into XML document. The XML document will be signed with a digital Signature and will be stored in a Sedna XML database. Then it will be sent to another laptop/Android Phone using Internet. At the receiver end the data is retrieved and verified. And when the receiver will receive this verified secure and authenticated signal with showing the result, the doctors can diagnosis the disease.

A. Proposed Model of ECG System with XML Digital Signature

This Internet-based scalable system integrates multiple hospitals, mobile medical specialists and local mobile units/clinics to form a large virtual enterprise. The current version of the telemedicine system is based on the push model—patient's biomedical signals after parsed into XML document are digitally signed with a private key and saved in the XML data base. Then the signed XML doc is sent to an appropriate doctor.

Health workers carry ECG circuit device for measuring ECG. These ECG circuit devices are connected with a Smartphone/Laptop/Notebook, which uploads the data into the local medical center database server (Sedna XML DB). The medical center sends the request through internet connection to the nearest available doctor. The signature is verified at the receiver end . The receivers have the public key to decrypt the data. After decrypting the signature a hashed value will be found. Now the provided data will be again hashed with the same algorithm and match with the previously found hashed value. If these two hash values are same then the doctor is confirmed that the data sent from medical center is not modified by any third party.

The doctor then makes an evaluation of the measured data and provides consultations by telephone/Internet.Fig.2 shows this new and advanced ECG System with XML Digital Signature.

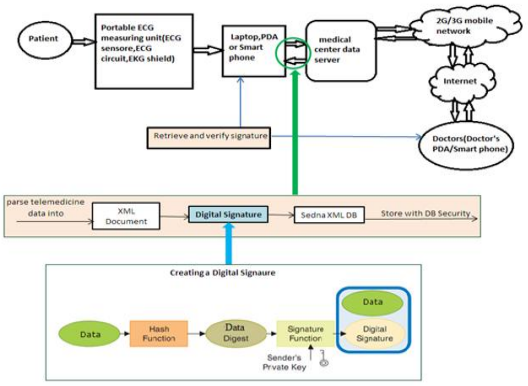

Fig.2.ECG System with XML Digital Signature

DOI 10.17148/IJARCCE.2015.4490

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

V. SYSTEM REQUIREMENT

For implementation, the system prerequisites are:
1) PortableECG measuring Units,
2) Local Medical Server,
3) LocalMedical Terminal,
4) Rural Medical Destination Terminal,
5) ECG Protocol Medical Data for Health Monitoring[9].

Tools used in this work for XML digital signature for ensuring the security and privacy of telemedicine data are XCA ,Java, Sedna API, Signature**.**

*1)XCA:*Is software to create certificate which obtains two essential data, a private key and a public key. They are generated as a key pair.

To sign the document the sender will sign the document with the private key retrieved from the certificate. After signing the document the document will be saved into database for distribution.

Obviously the certificate has to attach so that the receiving end can get the public key for verification.

*2)Java:*The jdk1.7.0 and jre7 is used to handle the full implementation of the system.

*3)SednaAPI:*For this Research the Java sedna-xmldb-api-261012 and sedna-xqj-api has been implemented here. Here we have introduced a much more simple database, Sedna , a XML based database.

This database is much simpler than MSSQL. Querying is also easier and you don't need to take care of the relation of different table .In a single table we can save information of several patient.

The basic structure of Sedna XML database stores the data in XML format. So the Database is simple a XML document [10].

*4)Signature:*XML Digital Signature is created by signing the XML doc get by the object of XMLDocument.

For this xml-security-1_5_3 API from Apache Software Foundation, Bouncy Castle Provider 15-134 API have been utilized. Major algorithms followed in this research are RSA and DSA:

*1)RSA(Rivest, Shamir, Adleman):*The signature schemes are defined in ANSI X9.31 - 1998 and in RSA PKCS #1 v2.1. Guidance for implementation can be found in FIPS 186-3 2006 (Digital Signature Standard (DSS)) is used to create digital certificate using XCA and to prepare a signed document.

2)Digital Signature Algorithm (DSA): This signature scheme is defined in FIPS 186-3(Digital Signature Standard (DSS)) is used to create/verify the document.

TABLE 1: PATIENT DATA/ECG ACQUISITION DATA [9]

ID	CONTENTS	LENGTH	VALUE(Parameter Data)
1	Name	1-15	String
2	Age	1-3	Number
3	Weight	1-3	Number
4	Height	1-3	Number
5	Patient ID	1-5	Number
6	Drugs	200	String
7	Heart Rate	20	Alphanumeric
8	Blood Pressure	30	Alphanumeric
9	ETT(exercise tolerance text)	300	Alphanumeric
10	Echo(2D & 3D mood) cardiac grapy	300	Alphanumeric
11	Cardiac Angiogram	300	Alphanumeric
12	Operational Mood	1	(Binary)[Basic(0), Emergency(1)]
13	Cardiac Enzyme –troponiu I & CK.MB (creatine kinase, myocardial band)	300	Alphanumeric
14	Medical Allergy or Drug Allergy	3-1000	(Binary) *Byte* *Contents* 1binary: set equal to 255 0-Unspecified, 1-Penicillin,100 others
15	Food Allergy	3-1000	(Binary)
16	SPO2(saturation of partial oxygen)	50	Alphanumeric

TABLE 2: DATA OF GENERATE ECG SIGNAL [9]

ID	CONTENTS	VALUE(Parameter data)
1	Patient ID	Number
2	Voltage(Heart muscles generate different voltages)	Binary
3	Time(sec)	Time

VI. SYSTEM DESIGN

The proposed system is a push system and the user interface designed by Eclipse. For our system we have used only a few patients information with their ECG data .When the Medical Center Server finds new data (ECG) of a patient, then all the information will be parsed using SAX parser into an XML doc. Before that the medical center and doctor is provided the certificate which is issued by a CA (Certification Authority). The certificate is provided by a file path. From the file path the system is taking the private key and the corresponding public key. After creating Document doc, the doc is then signed using the private key. To create a digital signature, first the data is hashed, which is to be signed using a cryptographic hash function. One commonly used hash function is SHA-1, which produces a 160-bit hash value is used for this purpose. The next step is to sign the hash value using a signing DSA algorithm and the private key. The equation is[11] :

Hash the data = H(M)(1)
Encrypt the hash of the data with private key =E(H(M))(2)
Signature = Eprivatekey(H(M))
Signed data=E(H(M))+M(3)
here,Key Pair = {PrivateKey, PublicKey};Data = M;Hash = H;Encryption = E;

Last of all we get a signed XML doc. Now the Document and original data(signed data) is then send to the Sedna database using XQuery by using the XQJ API. The public key is attached with the doc so that the verifier can decrypt the signature. The doctor retrieves the doc from the Sedna using XQuery. As the public key is attached with the document, the verification will be done internally by using the public key and the same hash algorithm (DSA) . If any changes occur in the signed XML document during data transmission the verifier will alert the doctor, that the signature is invalid. And if no changes have been occurred

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

by any third party the doctor will get the whole information of the patient data with a an alert that the document is signed by the specific medical center.And the next step equation is[11]:

Decrypt the hash of the data with public key = D(E(H(M)))+M=H(M)+M(4)
Hash the received original data =H(M)(5)
Match outcome 4 and 5 ,H(M)=H(M)(6)
Here,D=Decrypt.

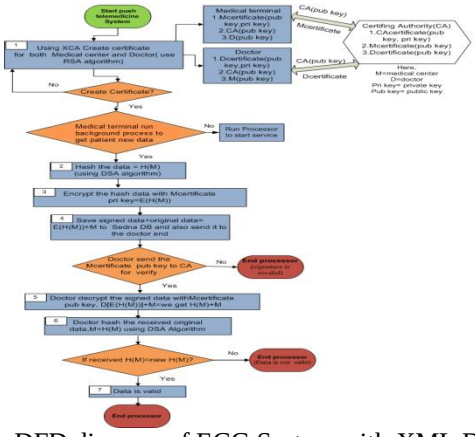

Fig.3. DFD diagram of ECG System with XML Digital Signature

Fig.4.Use Case diagram of the ECG System with XML Digital Signature

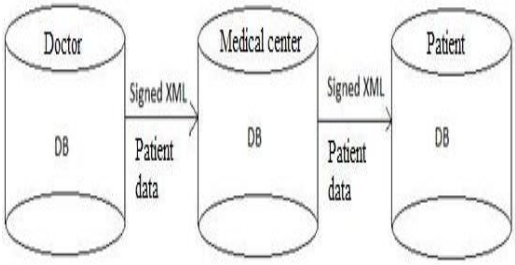

Figure 5: Transaction model of the ECG System with XML Sedna

VII. SYSTEM OUTCOME

If new patients are in database, doctor can see the total number of patient's details through the "teemed apps". Fig.6. Shows the patient details where at first stage Fig.6(a) shows the number of patients .Patient ECG acquisition data could beseen in next stage at Fig.6(b) and the last stage at Fig.6(c)shows the patient ECG curve. When doctor checks the patientit will be automatically removed from the queue. There is no chance to be attacked by the third party into this data as the data are digitally signed. The doctor can simply verify the document by using the public key that is attached with this document. Querying is also simpler in this case. The important thing is that all the user of this system as the doctoror the medical center, all has to get certificate from a certifying authority.

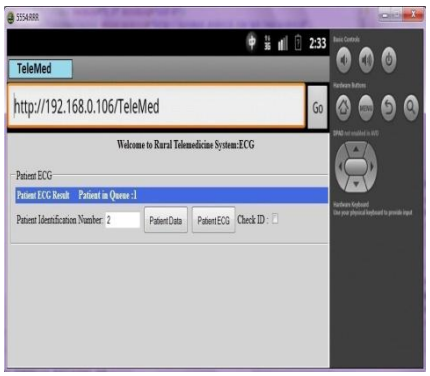

Fig.6(a).System screen shot of patient in queue

Fig.6(b).System screen shot of patient data

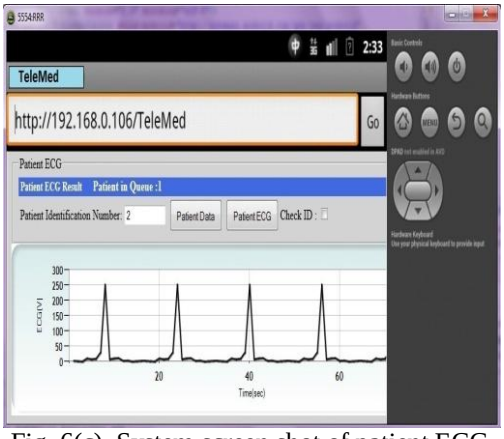

Fig. 6(c). System screen shot of patient ECG

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

VIII. PERFORMANCE ANALYSIS

In this section, we analyze the performance of proposed scheme. We have tested the security threat handling efficiency our proposed ECG System with 30 sample ECG medical records and compared the outputs from both traditional ECG telemedicine system and our proposed new ECG system with XML Digital Signature. Results are shown in TABLE 3.

TABLE 3

Telemedicine System	Failure of security threat handling	
	Out of 30 sample ECG medical records	%
Traditional ECG Telemedicine System without any advanced security mechanism	6	20
Proposed new ECG Telemedicine system with XML Digital Signature.	1	3.33

IX. LIMITATIONS

For telemedicine data transmission in a secured way we used the XML Digital Signature and Sednadatabase. Still there are some scope for improvements and optimizations because of some limitations in the present system.XML databases may need to be restructured before data conversion. Following that, Digital Signatures are an additional cost which should be weighed against their potential security benefits. User training may be needed in the system installation stage which would increase the one-time implementation cost and time. Additionally, as with all computer-related applications, sooner or later there will be a hiccup in the system and someoneneed to troubleshoot it which may not always possible in rural locations.

X. CONCLUSION

A secure mobile telemedicine system for local medical center is network-based and distributed information system to connect local patients to medical specialists. Therefore, it indicates to consider data security and inter-operability of telemedicine systems in remote area. Regarding device connectivity to the local medical server, the portable ECG measuring units have the advantage of being easily connected to a local terminal and that composed in the host medical server. The execution time of retrieving the data and verifying the signature is lower than the Traditional System[11].To execute the medical data in Sedna using Digital Signature , takes only 3ms.However considering network connectivity between a local medical server and aremote data server, more sophisticated system architecture is required in terms of data formats and communication protocols. Our future concentration will be on trying to minimize the risks and to develop an improved, optimized architecture with backup data center.

ACKNOWLEDEMENT

Authors were supported by the Department of Computer Science and Engineering, Jahangir nagar University, Savar, Dhaka, Bangladesh.

REFERENCES

[1]. M. Salajegheh, Molina, A., & Fu, K. "Home Telemedicine:Encryption Is Not Enough.", Journal Of Medical Devices, 3, 2009.
[2]. R. F. Olanrewaju, Nor'ashikin Bte. Ali, Othman Khalifa, Azizah AbdManaf, "ICT in Telemedicine: Conquering Privacy and Security Issues In Health CareServices".
[3]. Natalie Armstrong , John Powell , Hilary Hearnshaw , Jeremy Dale , "Design of a trial of Internet-based self-management for diabetes ",Journal of Telemedicine and Telecare,. 2007;13 Suppl 1:1–2.
[4]. Barlow J, Singh D, Bayer S, Curry R.," A systematic review of the benefits of home telecare for frail elderly people and those with long-term conditions." Journal of Telemedicine and Telecare. 2007;13(4):172–9.
[5]. Anastasios Fragopoulos, John Gialelis and Dimitrios Serpanos,"Security Framework for Pervasive Healthcare Architectures Utilizing MPEG 21 IPMP Components",International Journal of Telemedicine and Applications. 2009;2009:461560.
[6]. C. Busch, F. Graf,, S. Wolthusen, and A. Zeidler, "A System ForIntellectual Property Protection". Fraunhofer Institute, 4th World Multiconference on Systemics, Cybernetics and Informatics 2000.
[7]. R.F. Olanrewaju, O.O. Khalifa A. Abdalla and A.A Aburas,"Damageless Digital Watermarking Using Complex-ValuedArtificial Neural Network", Journal of Information &Communication Technology, Vol 9, pp.111-137, 2010, ISSN 1675-414X.
[8]. J. Zain, and M. Clarke, "Security In Telemedicine: Issues InWatermarking Medical Images", 3rd International Conference:Sciences of Electronic,Technologies of International and Telecommunications.March 27-31,2005,Tunisia
[9]. UmmeSaymaBusra, Mohammad ZahidurRahman, "Mobile Phone Based Telemedicine Service for RuralBangladesh: ECG", in Proc. of IEEE Intl. Conf. on Computer and InformationTechnology (ICCIT),p.203-208,March 8-10 , 2014 ,khulna, Bangladesh.
[10]. Maxim Grinev, AndreyFomichev, Sergey Kuznetsov ,"Sedna: A Native XML DBMS", Institute for System Programming of the Russian Academy of Sciences B. Kommunisticheskaya, 25,Moscow 109004, Russia, 2004.
[11]. Md. Momin Reja, "XML Digital Signture with Sedna", MSc. thesis, Dept of CSE,Jahangirnagor University, 2013
[12]. Vaibhav Garg, Jeffrey Brewer, "Telemedicine Security: A Systematic Review", Journal of Diabetes Science and Technology, Vol 5(3), 2011 May; 5(3): 768–777. Published online 2011 May 1