ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

A Secured Software Architecture for Providing Data Security in Cloud

K.Venkatraman[1],G Maria Kalavathy[2]

Research scholar, Anna University Chennai, India[1]

Professor, St.Joseph's College of Engineering Chennai, India[2]

ABSTRACT: This paperaims at providing security and preserving the privacy of the patient information while it is being transferred from one location to another. This paperalso implements fine grained access privileges to patient information. We consider first-order linear temporal logic (LTL) techniques for user creation and setting user privileges. It is an appropriate formalism for specifying RBAC policies because as often, one must cope with dynamic policies. The patient information is encrypted by using Data Encryption Standard (DES) algorithms. The 56 bit key size of DES ensures that the chances of the intruder identifying the key are difficult. The series of internal transformations is the strength of this algorithm.The proposed method to apply the Probabilistic Packet Marking algorithm is used to calculate the checksum value. The approach to IP traceback is based on the probabilistic packet marking paradigm. The IP trace back technique is used to verify the checksum value to trace the attacking IP address and preserve the privacy of patient information.

I. INTRODUCTION

Recently, with the rapid development in wearable medical sensors and wireless communication, wireless body area networks (WBANs) have emerged as a promising technique that will revolutionize the way of seeking healthcare, which is often termed *e-healthcare*. Instead of being measured face-to-face, with WBANs patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, and insurance companies.

In this way healthcare processes, such as clinical diagnosis and emergency medical response, will be facilitated and expedited, thereby greatly increase the efficiency of healthcare. Based on the WBAN, a wide range of novel applications are enabled, such as ubiquitous health monitoring (UHM), computer-assisted rehabilitation, emergency medical response system (EMRS), and even promoting healthy living styles. Specifically, in UHM the WBAN frees people from visiting the hospital frequently, and eases the heavy dependence on a specialized workforce in healthcare. Thus, it is a desirable technique to quickly build cost-effective healthcare systems, especially for countries that are short of medical infrastructure and well trained staff.

1.1 PROBLEM DEFINITION

Since the patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of these data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments. In reality, patient- related data is often stored in a distributive manner; the open and dynamic nature of the WBAN makes the data prone to being lost. Therefore, it is equally important to protect patient-related data against malicious modification and to ensure its dependability (i.e., having it readily retrievable even under node failure). Meanwhile, we must address various privacy concerns that may hinder wide public acceptance of WBAN technology.

Especially access to patient-related data must be strictly limited only to authorized users; otherwise, the patients' privacy could be abused. As a governmental initiative, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has specified a set of mandatory privacy rules to protect sensitive personal identifiable health information. However, in WBANs distributive stored private data may easily be leaked due to physical compromise of a node. Therefore, data encryption and cryptographically enforced access control is needed to protect the privacy of patients. To design data security and privacy mechanisms for WBANs, there are a number of challenges one must overcome, including how to make tough balances between security, efficiency, and practicality.

II. LITERATURE REVIEW

1. Data Security and Privacy in Wireless Body Area Networks

The wireless body area network has emerged as a new technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices, and the high demand for both security/privacy and practicality/usability. In this article we look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. We discuss various practical issues that need to be taken into account while fulfilling the security and privacy requirements.

Relevant solutions in sensor networks and WBANs are surveyed, and their applicability is analyzed.

2. Probabilistic Packet Marking for Large Scale Ip Traceback

This paper presents an approach to IP traceback based on the probabilistic packet marking paradigm. Our approach, which we call randomize-and-link, uses large checksum cords to "link" message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages.

3. Analyzing and Managing Role-Based Access Control Policies

Today, more and more sensitive data is stored on computer systems; security-critical business processes are mapped to their digital counterparts. This situation applies to institutes that have different security requirements, such as the healthcare industry, digital government, and financial service institutes. Authorization constraints help the policy architect design and express higher level organizational rules. Although the importance of authorization constraints has been addressed in the literature, a systematic way to verify and validate authorization constraints does not exist. In this paper, we specify both non-temporal and history-based authorization constraints in the Object Constraint Language (OCL) and first-order linear temporal logic (LTL). Based upon these specifications, we attempt to formally verify role-based access control policies with the help of a theorem prover and to validate policies with the UMLbased Specification Environment (USE) system, a validation tool for OCL constraints. We also describe an authorization engine, which supports the enforcement of authorization constraints.

4. A temporal-logic extension of role-based access control covering dynamic separation of duties

Security policies play an important role in today's computer systems. We show some severe limitations of the widespread standard role-based access control (RBAC) model, namely that object-based dynamic separation of duty as introduced by Nash and Poland cannot be expressed with it.

We suggest overcoming these limitations by extending the RBAC model with an execution history. The natural next step is then to add temporal logic for the specification of execution orders. We show that with this, object-based dynamic separation of duty, as well as other policies, can be adequately specified.

III.PROPOSED SYSTEM

Proposed system address the Data Storage Security Requirements namely Confidentiality, Dynamical integrity assurance, Dependability.Further the proposed system also focuses on data access security requirements namely Access control (privacy),Accountability, Revocability, Non-repudiation

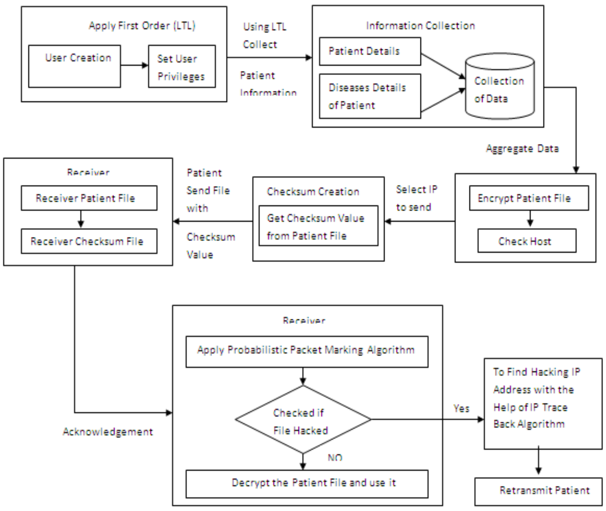


Fig: 3.3.1.1 System Architecture

3.4 IMPLEMENTATION

IP Trace:

In this module we can retrieve all system name and IP address. This is useful to find which systems are active or inactive. We can send data to active system through LAN.

Client:

We can send data from client to selected server. The client have to calculate the checksum for selected file and can view the checksum values. It must display only in number format.

Packet Marking:

The client can mark the packet use the function may be expressed as

$A = 1 + D1 + D2 + ... + DN \pmod{65521}$

$B = (1 + D1) + (1 + D1 + D2) + ... + (1 + D1 + D2 + ... + DN) \pmod{65521}$

$B= N\times D1 + (N-1)\times D2 + (N-2)\times D3 + ... + DN + N \pmod{65521}$

$D = B * 65536 + A$

where D is the string of bytes for which the checksum is to be calculated,and N is the length of D.

Server :

The server selects the path to receive the data from client. The server receives the packet and checksum .The checksum value only in notepad format in shared folder.

Verify Checksum:

The server also calculates the checksum value for received data from client. In this module compare the two checksum value, if it’s not equal the hacker has changed the packet, if it’s equal no change in received packet.

Acknowledgement:

In this module, if the server received the packet with checksum then it sends acknowledgement to client through local area network.

Techniques and Algorithm:

Linear Temporal Logic: We consider first-order linear temporal logic (LTL) as an appropriate formalism for specifying RBAC policies because, often, one must cope with dynamic policies. In banking applications, for example, dynamic SoD (separation of Duty) authorization constraints must be enforced, such as history-based SoD. History-based SoD is a flexible variant of SoD, in which a user may have all the privilege for a business process but must not perform all the subtasks of this process on a certain object (e.g., check).

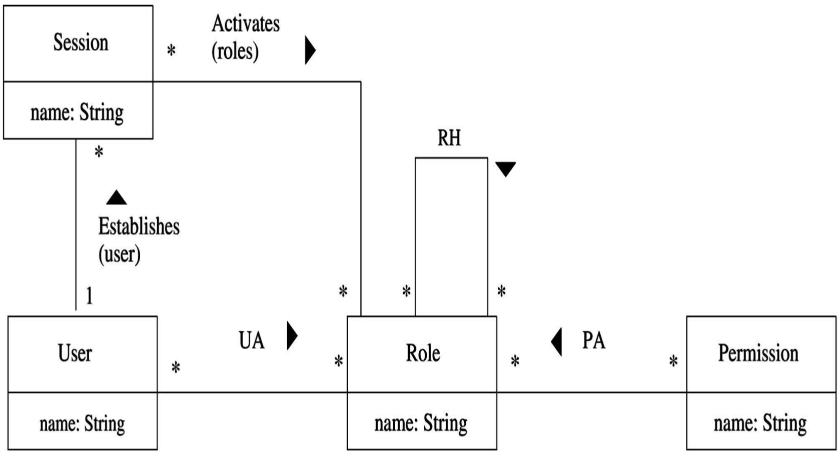


Fig: 3.5.1 Linear temporal Logic

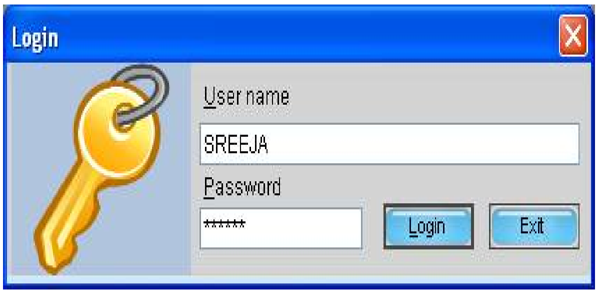
Probabilistic packet marking algorithm:

The proposed method to apply the Probabilistic packet marking algorithm is used to calculate the checksum value. An approach to IP traces back based on the probabilistic packet marking paradigm. Our approach, which we call randomize-and-link, uses large checksum cords to "link" message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers.

IP trace back algorithm:

The IP trace back technique is used to check sum value to trace the attacking IP address. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Although the file will be easily detected by getting the Router's IP address a HMAC and the Key Revelation. After increasing the scheming it would allow for Fast and Efficient Trace back.

IV. RESULTS AND DISCUSSION



User name
SREEJA
Password
******

Fig: 4.2.1 Login Screen

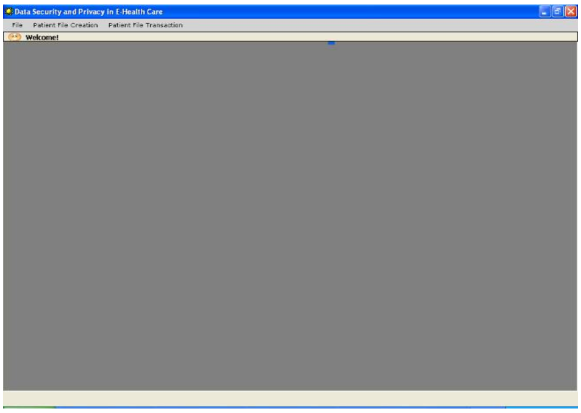
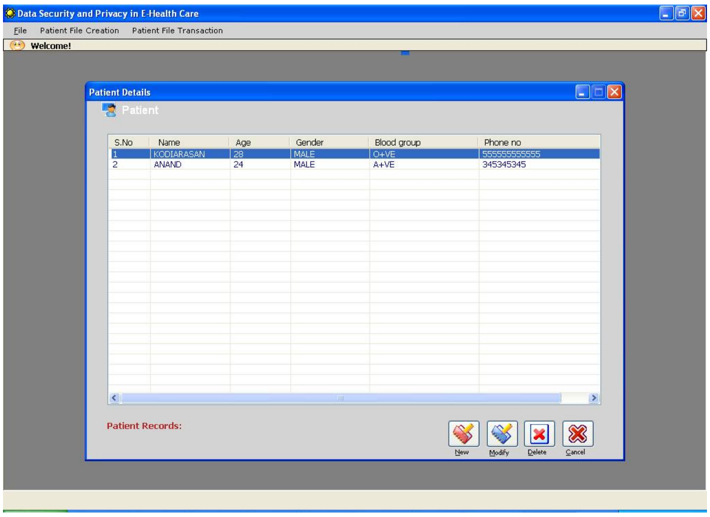


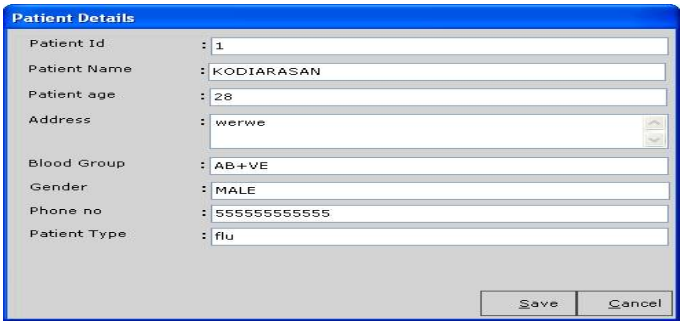
Fig: 4.2.2 Main Screen



S.No	Name	Age	Gender	Blood group	Phone no
1	KODIARASAN	28	MALE	O+VE	555555555555
2	ANAND	24	MALE	A+VE	345345345

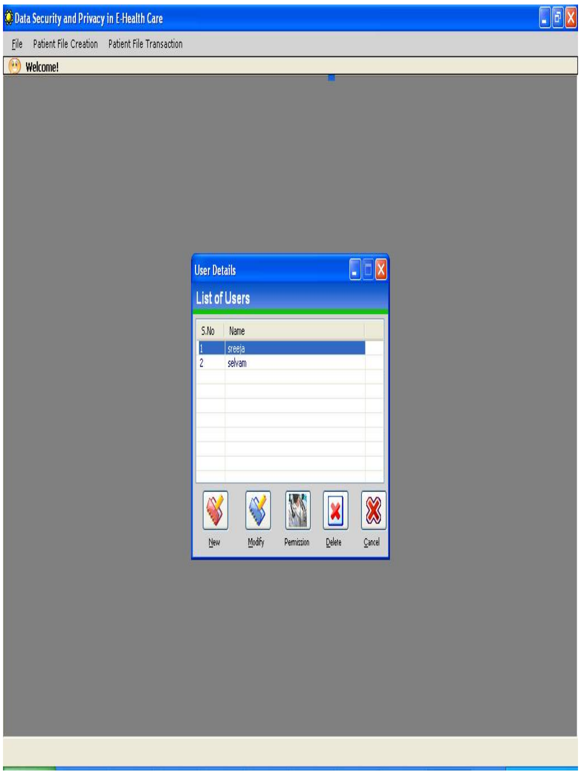
Patient Records:

Fig: 4.2.3 Patient Screen



Patient Id	:	1
Patient Name	:	KODIARASAN
Patient age	:	28
Address	:	werwe
Blood Group	:	AB+VE
Gender	:	MALE
Phone no	:	555555555555
Patient Type	:	flu

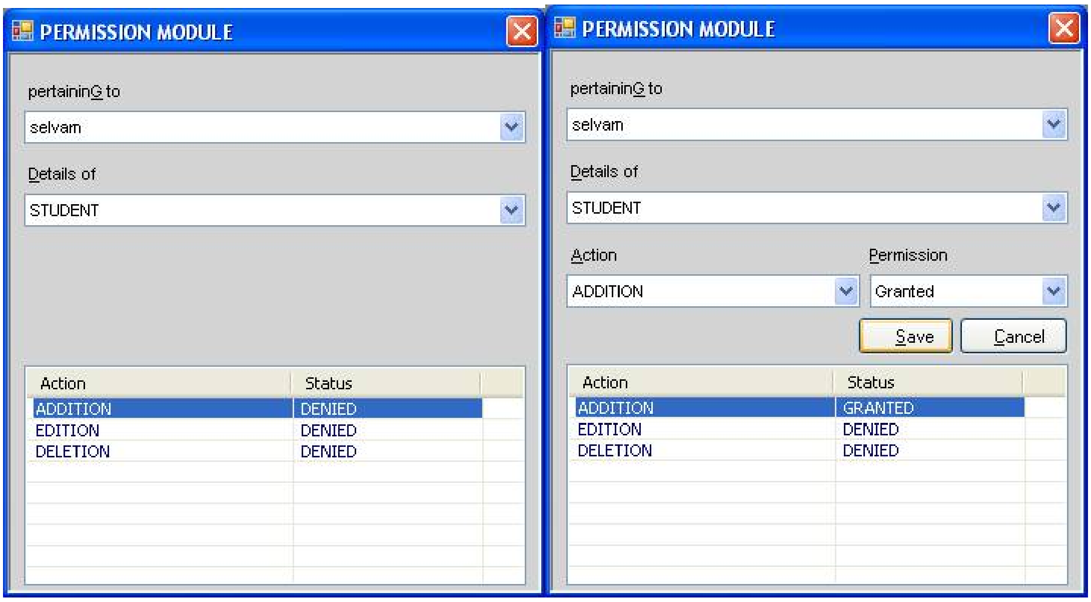
Fig: 4.2.4 Patient Details Screen



List of Users

S.No	Name
1	sreeja
2	selvam

Fig: 4.2.5 Users Screen



pertaininG to: selvam

Details of: STUDENT

Action	Status
ADDITION	DENIED
EDITION	DENIED
DELETION	DENIED

pertaininG to: selvam

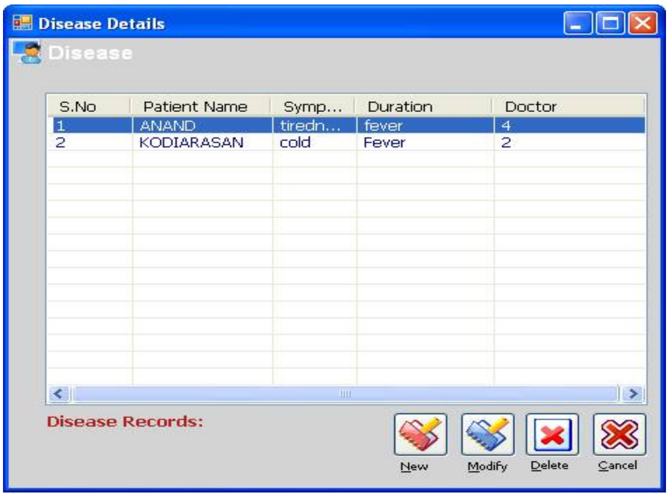
Details of: STUDENT

Action: ADDITION

Permission: Granted

Action	Status
ADDITION	GRANTED
EDITION	DENIED
DELETION	DENIED

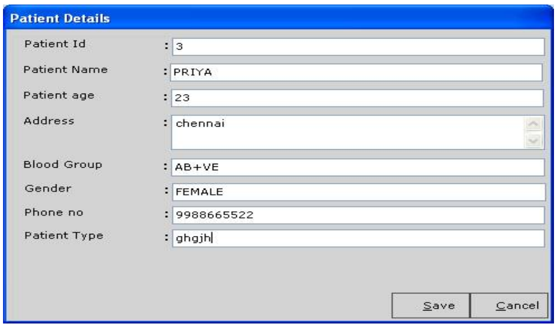
Fig: 4.2.6 Permissions Screen



S.No	Patient Name	Symp...	Duration	Doctor
1	ANAND	tiredn...	fever	4
2	KODIARASAN	cold	Fever	2

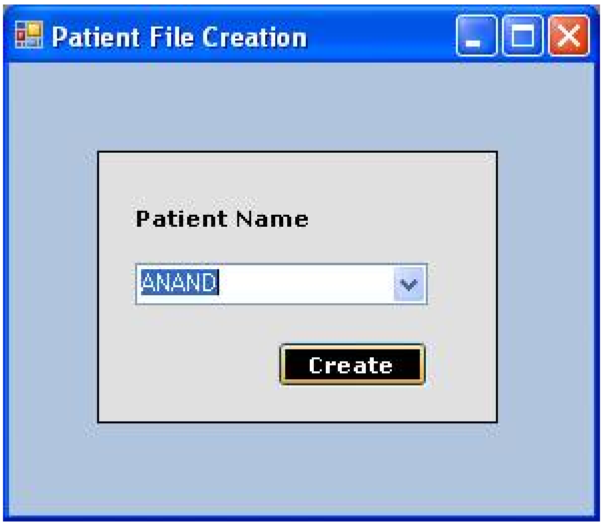
Disease Records:

Fig: 4.2.7 Disease Screen



Patient Id	: 3
Patient Name	: PRIYA
Patient age	: 23
Address	: chennai
Blood Group	: AB+VE
Gender	: FEMALE
Phone no	: 9988665522
Patient Type	: ghgjh

Fig: 4.2.8 Disease Details Screen



Patient Name: ANAND

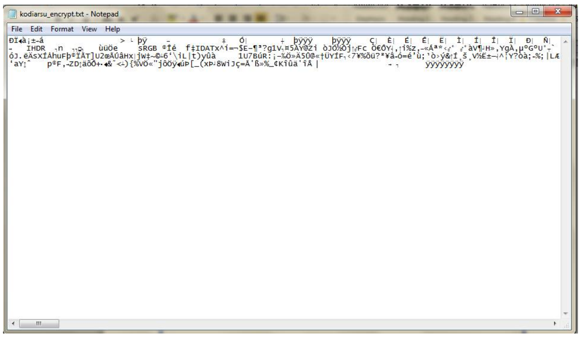
Fig: 4.2.9 Patient File Creation Screen

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

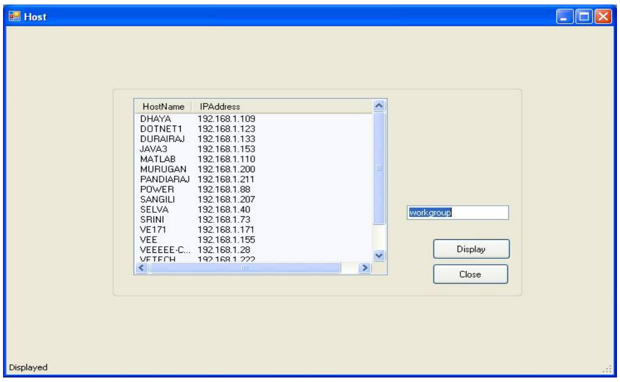
Vol. 6, Special Issue 3, November 2017



kodiarsu_encrypt.txt - Notepad

```
ÐÏ◂à¡±-á                    > └ þÿ    -         ♀   Ó|        ┼  þÿÿÿ    þÿÿÿ    Ç|  È|  É|  Ê|  Ë|  Ì|  Í|  Î|  Ï|  Ð|  Ñ|
→   IHDR  ┐n  ┐┐□┐   ùüÖe    sRGB ®Îé  f‡IDATx^í=¬$E–¶³?g1V┐¤5ÀY@Zi òJÓ½Ój↑♂Fc Ö€ÔY┤,↑i%z,-«Åª*‹♂° ♂°àV¶┘H»,YgÀ,µºGºU°┬`
óJ.ëÄsXÍÀhuFþ®ÏÀT]U2œÅÚâHx|jW‡~©┘6'\iL|t)yûà     1U7BúR:¡–%Ö»Ä5Ö@«†ÜYÍF┐<7¥%õü?²¥â┘ó=é'ù;'ò›ý&↑Í¸š¸V½Ë±—┤^¦Y?òà;┘%;|LÆ
'aY↑ˆ    p®F,┘ZD↑äõÔ+·◂&˜<┘){%VÖ«"jôÖÿ◂úÞ[_(xÞ┘8WiJç=Å'ß»%_¢KÎûä'îÅ |                 → ┐      ÿÿÿÿÿÿÿÿ
```

Fig: 4.2.10 Encrypted Patient File



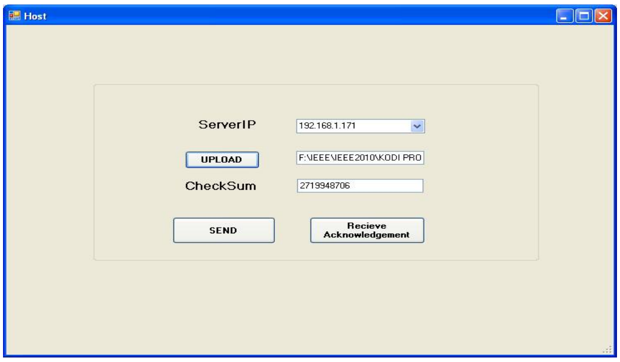
Host

HostName	IPAddress
DHAYA	192.168.1.109
DOTNET1	192.168.1.123
DURAIRAJ	192.168.1.133
JAVA3	192.168.1.153
MATLAB	192.168.1.110
MURUGAN	192.168.1.200
PANDIARAJ	192.168.1.211
POWER	192.168.1.88
SANGILI	192.168.1.207
SELVA	192.168.1.40
SRINI	192.168.1.73
VE171	192.168.1.171
VEE	192.168.1.155
VEEEEE-C...	192.168.1.28
VETECH	192.168.1.222

workgroup

Displayed

Fig: 4.2.11 Host Display Screen



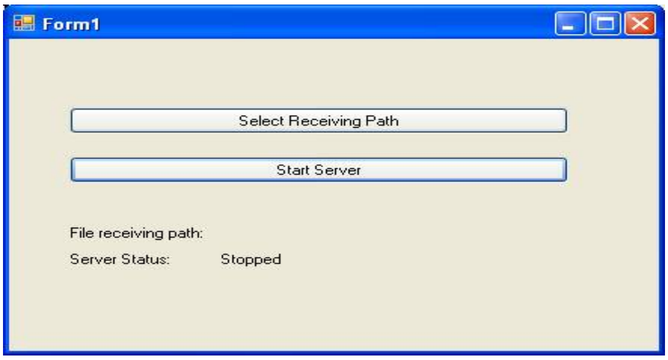
Host

ServerIP: 192.168.1.171

UPLOAD: F:\IEEE\IEEE2010\KODI PRO

CheckSum: 2719948706

Fig: 4.2.12 Sender Screen



Form1

File receiving path:

Server Status: Stopped

Fig: 4.2.13 Receiver Screen

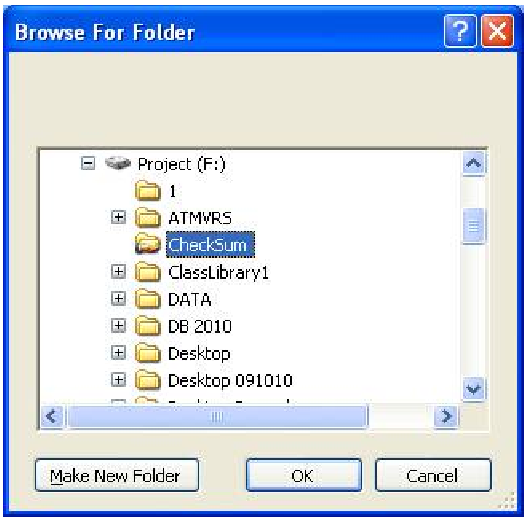
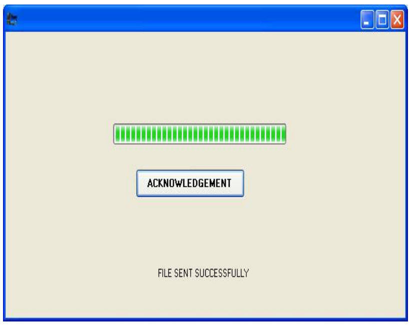


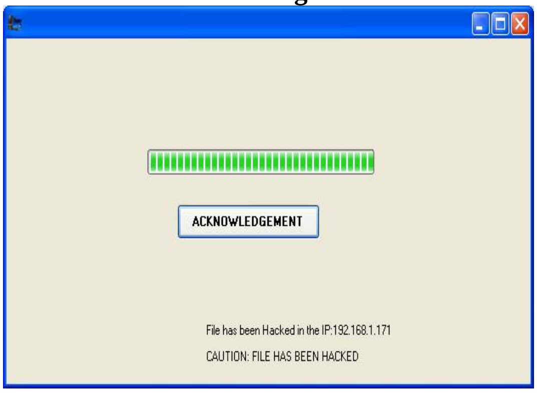
Fig: 4.2.14 Receiving Path Selection Screen



FILE SENT SUCCESSFULLY

Fig: 4.2.15 Acknowledgement

Second Time After Change Checksum Value:



File has been Hacked in the IP:192.168.1.171

CAUTION: FILE HAS BEEN HACKED

Fig: 4.2.16 Alert on Hacking

V. CONCLUSION

The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices, and the high demand for both security/privacy and practicality/usability

The WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. Data security and privacy in WBANs and WBAN-related e- healthcare systems is an important area, and there still remain a number of considerable challenges to overcome. The research in this area is still in its infancy now, but we believe it will draw an enormous amount of interest in coming years. We hope this paper will inspire novel and practical designs of secure, dependable, and privacy enhanced WBANs.

REFERENCES

[1] E. Jovanov *et al.*, "A Wireless Body Area Network of Intelligent Motion Sensors for computer Assisted Physical Rehabilitation," *J. NeuroEng. Rehab.*, vol. 2, no. 6, Mar. 2005.

[2] D. Halperin *et al.*, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Comp.*, vol. 7, no. 1, Jan. 2008, pp. 30–39.

[3] K. Lorincz *et al.*, "Sensor Networks for Emergency Response: Challenges and Opportunities," *IEEE Pervasive Comp.*, vol. 3, no. 4, Oct.–Dec. 2004, pp. 16–23.

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule; http://www.hhs.gov/ocr/ privacy/

[5] S. Chessa and P. Maestrini, "Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks," *Int'l. Conf. Dependable Sys. Net.*, June 2003, pp. 207–16.

[6] Q. Wang *et al.*, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," *Proc. IEEE INFOCOM '09*, Apr. 2009.

[7] R. Di Pietro *et al.*, "Catch Me (If You Can): Data Survival in Unattended Sensor Networks," *Proc. IEEE PerCom*, Mar. 2008, pp. 185–94.

[8] K. K. Venkatasubramanian and S. K. S. Gupta, "Security Solutions for Pervasive Healthcare," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Y. Xiao, Ed., Auerbach, 2007, pp. 443–64.

[9] O. G. Morchon and H. Baldus, "Efficient Distributed Security for Wireless Medical Sensor Networks," *Int'l. Conf. Intelligent Sensors, Sensor Net., Info. Processing*, Dec. 2008, pp. 249–54.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext- Policy Attribute-Based Encryption," *Proc. IEEE Symp. Security and Privacy*, May 2007.

[11] M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks," in *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51-58, February 2010.doi: 10.1109/MWC.2010.5416350.

[12] Probabilistic Packet Marking for Large-Scale IP Traceback, Michael T. Goodrich, Senior Member, IEEE IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. X, NO. X, JANUARY 2007