ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Ensured Patient Healthcare Monitoring in Cloud Infrastructure

M. Varnani Raj
M.Tech Student,
Dept of CSE,
Bheema Institute of Technology& Science.

V. Mallesi
Assistant Professor,
Dept of CSE,
Bheema Institute of Technology& Science.

ABSTRACT:

This cloud assisted mobile health monitoring includes mobilecommunication as well as cloud computing technologies to provide various services especially feedback decision support using information communication Technologies (ICT's) and mobile healthcare applications for the both parties involved in this mechanism for better security with extended privacy and data integrity by applying techniques. This system is to provide the simple user interface which can be easily understandable.

It incorporated the hash based message authentication code (MAC) and MD-5 algorithm technique which can protect data integrity. This system also uses AES algorithm and outsourcing decryption technique for better privacy and security. Proposed design demonstrates mobile healthcare applications with simple user interface and protection to integrity of data in cloud-assisted privacy preserving mobile health monitoring. This system provides easeful mobile healthcare applications with good results and it is very useful to remote area peoples where hospitals not easily accessible.

KEYWORD:

CAM System Design and Architecture, Algorithm for MD-5 Algorithm, PPSPC Framework.

I. INTRODUCTION :

Wide deployment of mobile devices, such as smart phones equipped with low cost sensors, has already shown great potential in imp roving the quality of healthcare services. Re mote mobile health monitoring has already been recognized as not only a potential, but also a successful example of mobile health (mHealth) applications especially for developing countries.

The Microsoft launched project "MediNet" is designed to realize remote monitoring on the health status of diabetes and cardiovascular diseases in re mote areas in Caribbean countries. In such a remote m Health monitoring system, a client could deploy portable sensors in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/ EKG), peripheral oxygen saturation (SpO_2) and blood glucose.

Such physiological data could then be sent to a central server,[3] which could then run various web medical applications on these data to return timely advice to the client.

A. The main contributions of this paper are:

1. User-centric privacy access control in opportunistic computing, we present an efficient attribute based access control and a novel non-homomorphism encryption based privacy preserving scalar product computation (PPSPC) protocol.

2. The effectiveness of this frame work in m-Healthcare emergency, we also develop a custom simulator built in Java. Extensive simulation results show that the proposed frame work can help medical users.

2. CAM SYSTEM DESIGN & ARCHITECTURE :

The new system uses various mobile health care applications by login as a registered user, the registration facility is provided by healthcare service provider's side. After using such user's specific application he/she sends health related data to the health service provider by using semi trust authority and on cloud server information gets stored which uses our newly proposed algorithm for data integrity and for extended privacy.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2. 1. Our proposed modification to protect data integrity using AES algorithm and MD5 algorithm (hash Function)

In this project AES algorithm used with MD5 algorithm (hash function) can be used as a digital signature mechanism. Message of arbitrary length and produces as output a 128 bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest.

Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP. AES cipher incorporates the following:

• Add Round Key() – round key is added to the State using XOR operation .

• Mix Columns() – takes all the columns of the State and mixes their data, independently ofone another, making use of arithmetic over GF(2^8) .

• Shift Rows() – processes the State by cyclically shifting the last three rows of the State by different offsets

• Sub Bytes() – uses S-box to perform a byte bybyte substitution of State[8, 9] .

Algorithm for MD-5 Algorithm :

Steps 1 – append padded bits:

The message is padded so that its length is congruent to 448, modulo 512. Means extended to just 64 bits shy of being of 512 bits long. A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.

Step 2 – append length:

A 64 bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.

Step 3 – Initialize MD Buffer

Step 3 cont.

Step 4 – Process message in 16-word blocks.

Step 4 count – Process message in 16-word blocks cont

Step 5 – output

Example :

The message digest produced as output is A, B, C, and D. That is, output begins with the low-order byte of A, and end with the high-order byte of D [9, 10].

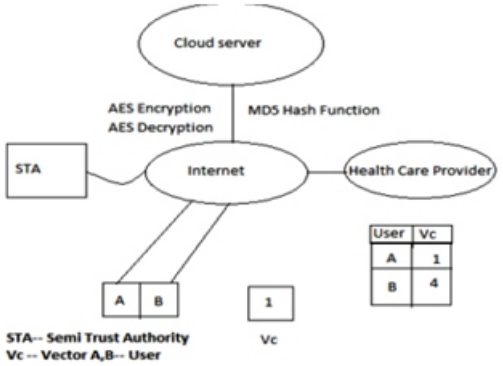

Fig.1 Our Modification to Protect Integrity

3. PROPOSED SYSTEM :

In this paper, we propose a new secure and privacy-preserving opportunistic computing frame work, called CAM, to address this challenge. With the proposed CAM frame work, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high reliability of process and minimizing privacy disclosure in m-Healthcare emergency. We introduce an efficient user-centric privacy access control in CAM frame work, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming data.

A. System model :

In health care responsible health care benefits of our system, a medical personnel at the center who is considered trustworthy is for initializing and controlling the entire system.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A user who wishes to get the mobile healthcare system registers himself as a medical user under a particular health care center, then a medical professional examines the user and generates his health profile. Based on the health profile, the users are then provided with the particular type of data such as heart rate, blood sugar level and other materials. Once being equipped with the sensors the users can move anywhere unlike in hospital.[1, 6 and 7] The sensors begin to collect the sensed data and transmit them to the user's smart phone which is then transmitted to the health care center. These smart phones play a vital role in mobile monitoring of patients. The smart phones are used for various purposes, the power of the smart phone may not be sufficient under emergency circumstances. Hence we make use of opportunistic computing where whenever a medical user is in emergency other medical users in the nearby area can contribute their resources.

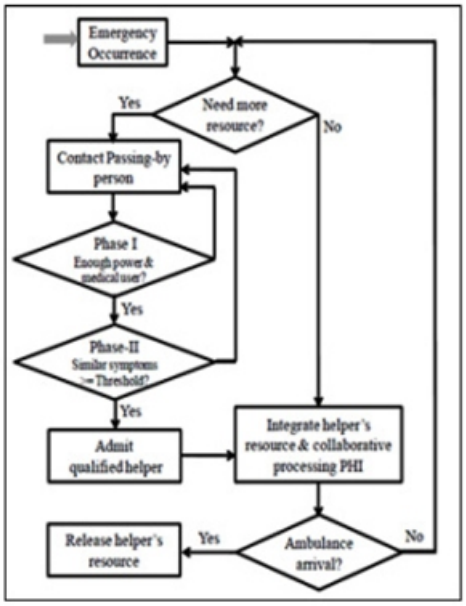

Fig.2. Opportunistic computing with two-phase privacy access control for m-Healthcare emergency.

A. PPSPC Framework :

In this section, we propose our PPSPC framework which focuses on initializing the system, the scenario depicting healthcare care monitoring under normal conditions and the health care monitoring during emergency situations.

B. Initializing the system :

According to our work, the person at the health care center is responsible for initializing the entire system. The authority at the health care center generates the bilinear parameters () by running gen(sp) using the security parameter (sp).He also selects the encryption algorithm that is to be used, two secure cryptographic hash functions H and H′, two random elements (h1,h 2) in G1 is choose also the master key is selected by choosing two random numbers (a, b) that belongs to Zq . Using the above elements the authority computes x=H(a),A=ga,e (g, g)b. The master key(a,x,b) is kept secretly and the remaining parameters are revealed parameter s=(q,g,G,GT,e,H,H',h1,h2,A.e(g,g) b, Encryption()). The medical user MUi is examined thoroughly and based on this a health profile is generated according to which the users are provided with sensors and the necessary medical software is installed in the users Smartphone.

C. Health Monitoring Under Normal Scenario:

The medical user MUi chooses the current date CD and computes the session key (ski), Ski=H(ki||CD) and is given to the sensors and Smartphone. The data, r data collected for every five minutes by the sensors are encrypted using the session key, Encryption (ski, r data||CD) to the Smartphone using Wi-Fi technology. The Wi-Fi technology increases the coverage. The Smartphone on receiving the encrypted data uses the session key(ski) to decrypt the data so as to process the rdata after which the data is sent to the healthcare center using 3G technology MUi||CD||encryption(ski, data||CD). The authority after receiving the processed data uses the master key (x) for computing MUi's secret key ki=H(MUi||x) and uses this to compute ski=H(ki||CD).This session key is used to recover the processed data data||CD fromencrypted(ski, data||CD). The date is corrected and the authority sends the processed data to the medical professionals.

D. Health Monitoring Under Emergency Situation :

When MUo faces an emergency such as abnormal raise in the heartbeat and becomes unconscious, then the authority at the healthcare center monitors all these changes and act to this situation immediately by sending the medical professional according to the medical user's need.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Before the arrival of the medical professional the user has to be monitored continuously for which the user's Smartphone requires high power for transmitting the user's health information due to which there are many chances that the resources in the user's Smartphone may not be sufficient. To find if a person passing by is a medical user the medical user MUo performs the following:

1. The user MU_0 chooses a random number $r \in Z_q^*$ and computes $e(g.g)^{br}$ and $c = (c_1.c_2.c_3)$ as $c_1 = g^r$ $c_2 = A^1.h_1^{-r}$ $c_3 = h_2^{-r}$
2. When another MU_j passes by the emergency location, MU_0 sends $c = (c_1.c_2.c_3)$ to the MU_j.

Once MU_j receives $c = (c_1.c_2.c_3)$ he performs the following

Uses his access control key

$ak_j = (g^{b+ar_{j1}}.g^{r_{j2}}.g^{r_{j2}}.h_1^{r_{j2}}.h_1^{r_{j2}})$ and computes the following

$$= \frac{s(c_1 g^{b-ar_{j1}})}{s(g^{r_{j1}}c_2).s(g^{r_{j1}}.c_2).s(h_1^{r_{j1}}h_2^{r_{j2}}.c_2)}$$

$$= \frac{s(g^r g^b g^{ar_{j1}})}{s(g^{r_{j1}}g^{ar}h_1^{-r})s(g^{r_{j2}}.h_2^{-r})s(h_1^{r_{j1}}.h_2^{r_{j2}}g^r)}$$

$$= \frac{s(g^r g^b).s(g^r g^{ar_{j1}})}{s(g^{r_{j1}}g^{ar}).s(g^{r_{j1}}.h_1^{-r}).s(g^{r_{j2}}.h_2^{-r}).s(h_1^{r_{j1}}.h_2^{r_{j2}}g^r)}$$

$$= \frac{s(g^r g^b)}{s(g^r.h_1^{r_{j1}}h_2^{r_{j2}}).1.s(h_1^{r_{j1}}.h_2^{r_{j2}}g^r)}$$

$$= e(g.g)br$$

Computes the H'(e(g,g)brts in which ts is the current timestamp and send back authentication || ts to MUo. After the user receives authentication || ts at timestamp ts', the user MUo checks the validity of the time interval between ts' and ts to prevent replay attack. If |ts'-ts| where is the transmission delay.MU o accepts authentication || ts and rejects otherwise then MUo uses the stored e(g,g)br to compute authentication' = h'(e(g,g)br|| timestamp) and checks authentication' = authentication if it fails, MU j is not authenticated as a medical user.

E. Analysis of benefits of opportunistic computing in mobile health care emergency :

In this section , we analyze the benefits provided by the opportunistic computing to a user who is at emergency.

Let us consider that the medical professionals will arrive after a time period t1 to help a user in emergency. Assuming that the users arrival follows a Poisson distribution {N(t1),t10} the rate of arrival of the user is taken as μ. The number of other users who are eligible to help a user at emergency is given as Nh(t 1)=no and the number of users who pass by that scenario but are not eligible to help is given as N (t1)=n1.Therfore the total number of users who arrive at the scenario before the arrival of the ambulance with the medical professionals between the time period to and t1 could be no+n1. The probability that a user arriving at time can help a user at emergency is P().

Theorem 1:

The number of medical users who are expected to contribute resources within

$$[t_0.t_1] \text{ is } E[N_h(t_1)] = \mu t_1 p \text{ Where } p = {}^1/_t \int_{t_0}^{t_1} p(\tau)\, d\tau$$

Proof:

The total users arriving within the time period [to,t1] is given as N(t1)=Nh(t)+N (t1)=no + n1 and the time is uniformly distributed in the time period [to,t1].while defining p=P{a user who arrives in[to,t1] is a eligible person to help| N(t1)=no+n1}, we have p=1/t1d .The users arrive independently and so P{Nh(t1)=no, N (t1)=n1 | N(t1)=n o +n1} will give the number of users who are qualified to help during the total no +n1 Bernoulli's experiment.

$$P\{ Nh(t1)=n0, Nh(t1)=n1\}$$

$$= \binom{n0+n1}{n0} p^{n0}(1-p)^{n1} e^{-\mu t1}\frac{\mu_1^{n0-n1}}{(n0-n1)!}$$

$$= \frac{(n0+n1)!}{n0!n1!} p^{n0}(1-p)^{n1}.e^{-\mu t1(p+1-p)}\frac{\mu_1^{n0}\mu_1^{n1}}{(n0-n1)!}$$

$$= e^{-\mu t1 p}\frac{(\mu_1 p)^{n0}}{n0!}\; e^{-\mu t1}\frac{(1-p)\mu_1(1-p)^{n1}}{n1!}$$

The above equation indicate that both Nh(and N () are independent Poisson process and their rate is and .Hence the number of users who are expected to help a medical user in e emergency by contributing their resources is given as

$$E[N_h(t_1)] = \mu t_1 p \text{ Where } p = {}^1/_t \int_{t_0}^{t_1} p(\tau)\, d\tau$$

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4. RELATED WORK :

The opportunistic computing has increased the great interest recently, and we have brie fly reviewed them which are related to our work [2], [4], [5]. In [4], Avenuti et al have introduced the concept of opportunistic computing in wireless sensor network which solves the problem of storing and executing an application incase if it exceeds the memory available on a single node. The application code can be partitioned in a number of simple modules that opportunistically cooperate to carry out a complex task And each node executes the provided application by running the given tasks and providing service to the neighboring nodes. In [5], Conti deals with the Opportunistic exploitation of (pools of) resources.

The nodes can be able to communicate even if a completed connected path never exits between them. Mobility of the nodes provides them the opportunity to communicate with each other. Each user can avail not only of the resources available on its own device, but can also on other resources of the environment. In [2] Pazzi provides that the health information is monitored by the Sensors the sensed data to the health center using neighbor nodes.

This can be transmitted to the health care center only when there is a proper cooperation between the neighbor nodes. Although [4] and [5] are important for understanding how the concept of opportunistic computing paradigm work when resources available on other neighboring nodes to complete the given task, they have not considered the security and privacy issues existing in the opportunistic computing .Different from all the above works, our proposed PPSPC framework aims at the security and privacy issues by providing encryption.

5. FUTURE WORK :

The Smart phones that are available today are open to every individual and can be programmed easily.

6. CONCLUSION L:

This paper discusses the importance of using a secure and privacy preserving opportunistic computing (CAM) frame work form-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of process and transmission in emergency. The security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

REFERENCES :

[1] Toninelli, R. Montanari, and A. Corradi, "Enabling secure service discovery in mobile healthcare enterprise networks," IEEE Wireless Communicat ions, vol. 16, pp. 24–32, 2009.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network," in Proc. BodyNets'10, Corfu Island, Greece, 2010.

[3] Y. Ren, R. W. N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," MONET , vol. 16, no. 6, pp. 683–694, 2011.

[5] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, "Wireless body sensor network using medical implant band," Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.

[6] A. V. Dhukaram, C. Baber, L. Elloumi, B. J. van Beijnum, and P. D. Stefanis, "End user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust, " in Proc. Pervasive Health, 2011, pp. 478– 484.

[7] E. De Cristofaro, S. Faber, P. Gasti, and G. Tsudik, "Genodroid: Are privacy-preserving genomic tests ready for prime time?" in Proc. 2012. [

8] Bruce schneier"Applied Cryptography" 2nd Edition published by John Wiley&SonsInc.

[9] William stallings "Cryptography and Network Security" 3rd Edition published by Pearson Education Inc and Dorling Kindersley Publishing Inc.

[10] National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication # HMAC, 2001.