Authorization For Wearable Biomedical Gadgets Monitoring System

Nallareddy Suchitra [1] , S.G.Sanjana[2] ,L.Raji[3], Dr K.Vijaya[4] , J.Swetha[5]

[1]Nallareddy Suchitra, R.M.K Engineering College, Chennai, Tamil Nadu
[2]S.G.Sanjana, R.M.K Engineering College, Chennai, Tamil Nadu
[3]L.Raji, R.M.K Engineering College, Chennai, Tamil Nadu
[4]Dr K.Vijaya, R.M.K Engineering College, Chennai, Tamil Nadu
[5]J.Swetha, R.M.K Engineering College, Chennai, Tamil Nadu

Abstract - *The cloud computing and IOT technologies have succeed a lot of attention amidst the human race over a past few years. But, the cloud and IOT experience a major security issue. The information stored in the cloud database have only some access to its end users but it is little hard to preserve from discrete service providers. The existing technologies face high computation and high communication cost which are vulnerable to active attacks, where its essentiality has been reduced in the real-world application. So, we propose a user based cloud authentication scheme for securing the stored medical data. The user and the wearable sensor node develops a mutual authentication and establish a secret session key for secure communications in the future. Hence, we use Real-Or-Random(ROR) model and Automated Validation of Internet Security Protocols and Applications(AVISPA) for securing the medical data and from attacks.*

Key Words: Wearable Device, Healthcare,Big Data, Cloud Computing, Authentication,Security.

1 .INTRODUCTION

The major concerns in cloud computing are security and confidentiality as users have limited access on the stored data at the distant locations managed by different service providers. These components can be used to build advanced components in future network. The Cloud and IoT are integrated as cloud IoT model where it can be used together to provide services including wearable healthcare applications. Nowadays, the people are very interested in buying wearable devices such as smart watches and bracelets, wearable sleep aid devices, Etc which are available in the market. In recent years, due to the advancement in the technologies the wearable gadgets has been used by the people in a tremendous way .Due to the high sampling rate in the wearable device the data produced from it needs to be stored and handled carefully at the cloud centric data server. A wearable sensor-based medical system includes various sensor devices that are flexibly worn on different parts of the body of a person , including into textile fiber, clothes, elastic bands or even these can be directly attached to the human body in case the devices are implantable medical devices like pacemaker. The wearable sensors measure physiological data like electromyography, electrocardiogram, body temperature, heart rate, blood pressure, arterial oxygen saturation (SpO2), etc. The advances in wireless communication has won against the geographical barriers. In this work, a scenario in the Cloud of Things Centric (CoTC) for a smart healthcare system is considered, where a set of wearable sensor nodes are embedded . Since IoT devices produce a large amount of non-structured or semi-structured data , the collected big data has three characteristics, such as volume, variety, and velocity. As the cloud offers virtually unlimited, on-demand storage capacity and cheap price, it is the most suitable and cost effective solution to deal with big data produced by IoT devices.

2. RELATED WORK

2.1 Wearable Biomedical Parameter Monitoring System

There are some blind patients in one ward; also elder patients are there so it could not be handled by one caretaker or doctor. Hence to overcome these shortcomings creation of Wearable technique is introduced. The necessities of the system are that every patient should wear this band which would be connected to doctors 2018 computer server microcontroller via internet. The development of remote healthcare monitoring system is done by programming the r for making a wearable device using patient's physiological parameters which are logged at that instance and activity of patients can be viewed at the doctor's screen.

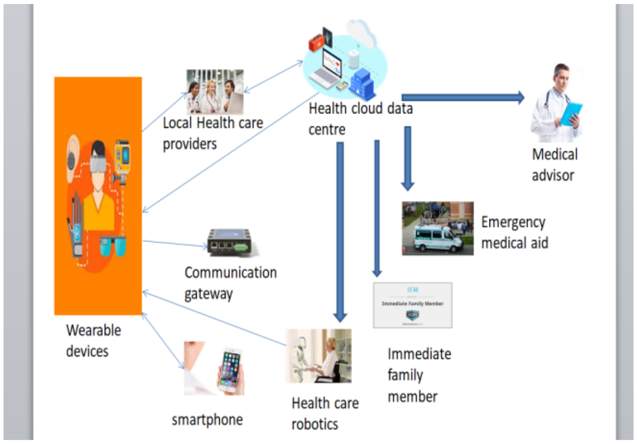
2.2 A health remote monitoring application based on wireless body area networks

Among the important research projects much deployed in healthcare field there is the wireless body Area networks (WBANs) applications, which can widely help to remote monitor the human health. This research aims to develop a wearable WBAN application for health remote monitoring, that monitor patient's health through the continuous detection, process and communicate of human physiological parameters. This application use four biomedical sensor nodes that are able to measure physiological signal (ECG, SPO2, heart rate and breathing) and convert it to useful data. Then, the data is transmitted by a processor and then sent to a central node by a transceiver. The data is collected and send to monitoring pc in real time, which projects and records the physiological parameters on a graphical interface.

3. PROPOSED SYSTEM

This paper introduces a cloudlet based healthcare system. The body data gained by wearable gadgets are sent to the nearby cloudlet. Those data are further sent to the remote cloud where doctors can access for disease diagnosis. According to data delivery chain, we divide the security form into three stages. Initially, user's necessary signs collected by wearable gadgets are sent to a closet gateway of cloudlet. During this process, data security is the main problem. In the next stage, user's data will be further sent toward remote cloud through cloudlets. A cloudlet is gathered by a certain number of mobile devices whose owners may need and/or share some specific data contents. Thus, both security and data sharing are considered in this stage.Especially, we use trust model to test trust level between users to determine sharing data or not. Based on the medical data stored in cloud,we provide security policy and protection. We also use collaborative IDS to protect cloud ecosystem in cloudlet mesh.

4. ARCHITECTURE DIAGRAM



5. METHODOLOGIES

5.1 SETUP PHASE

This phase comprises the following steps: Step 1. The BRC first chooses a long-term secret session key K for the Cloud of Things Centric (CoT C). The BRC then picks a unique identity and a unique master key for each deployed wearable sensor node. After that the BRC calculates the secret key and the corresponding secret credential for each wearable node. Step 2. The BRC also selects a cryptographic collision resistant one-way hash function h. Moreover, the BRC generates two distinct large primes p and q, and calculates the modulus n = p × q, where p and q are secret with the BRC and CoT C. Step 3. Finally, the BRC stores the information in CoT C's database.

5.2 REGISTRATION PHASE

The registration phase deals with both the user and the patient. This phase takes place only in offline mode and it is a one-time procedure.Medical Professional

Registration Phase: Step1:User first picks his/her identity & password on his/her choice, and then generates two random numbers. The user then computes pseudo-identity, pseudo password. After that the user dispatches the registration request to the BRC securely. Step 2: The BRC chooses a 160-bit random number for User . Step 3. The BRC generates a 160-bit secret key to be used between User and all the deployed sensor nodes . After that the BRC calculates the temporal credential T for each sensor node . In addition, the BRC generates a 160-bit secret key to be shared between user and CoT C, and also calculates the temporal credential for User . The BRC generates a smart card with the information and delivers it to user securely. Step 4 . After receiving smart card for the user securely, it stores all the information in the memory.

User Registration Phase: In this phase, a patient first selects and forwards his/her name to the BRC. The BRC then selects appropriate sensor kits and appoints a medical professional. Finally, the BRC forwards patient's identity and the required information of sensors to the appointed medical professional so that the user can acquire the live data from the wearable devices that are worn by the patient.

5.3 PRE-DEPLOYMENT

This phase is performed by the BRC in offline mode. Finally, the BRC stores the information in the cloud server.

5.4 LOGIN AND AUTHENTICATION PHASE

In this phase, the participants (user, cloud, wearable sensor node) are mutually authenticated each other, and at the end, a session key is established between user and node . The details are presented as follows: Step 1. User inserts smart card in a specific terminal and then provides identity & password into the smartcard reading device as inputs. If the verification fails, Smart card rejects the login request; otherwise, it proceeds to the next step. Step 2. Smart card selects an accessed sensor identity , generates current timestamp to undergo the calculations , and then dispatches the login request message to CoT C openly. Step 3.On successful verification, CoT C decrypts using the secret parameters p and q with the help of the Chinese Remainder Theorem (CRT) to retrieve. If there is no match found, CoT C aborts this phase. If the verification fails, CoT C rejects the login request. Otherwise, CoT C moves to the next step. Step 4. CoT C then computes and fetches the timestamp corresponding to identity and generates a random nonce and current timestamp to compute key and then transmits the authentication request message 2. Step 5. Sensor node also generates a random nonce and current timestamp T3 for the purpose of computing a session key shared with User , and then dispatches the authentication reply message to User via public channel. Step 6. On receiving Message from Sensor node , User first checks . Here the receiving time of Message is T ∗ 3 . Step 7. If the above verification fails, the process is terminated. Thus, at the end of this phase, both User and Sensor node reserve the same session key for communication securely.

5.5 PASSWORD CHANGE PHASE

This phase is executed by a registered medical professional (user) in order to change his/her current password by a new password. The following steps are essential to complete this phase: Step 1. User first inserts his/her smart card into a smart card reader and then provides identity and current password as inputs. Smartcard then calculates Pseudo identity, pseudo-password and verifies . If this verification fails, Smart card terminate this process. Otherwise, Smartcard asks user to input new password and continues to the next step. Step 2. User picks a new password and supplies to Smartcard . Smart card computes new pseudo-password. Step 3. User updates Register , Session key respectively. Finally, the smart card contains the information.

5.6 SMART CARD REVOCATION PHASE

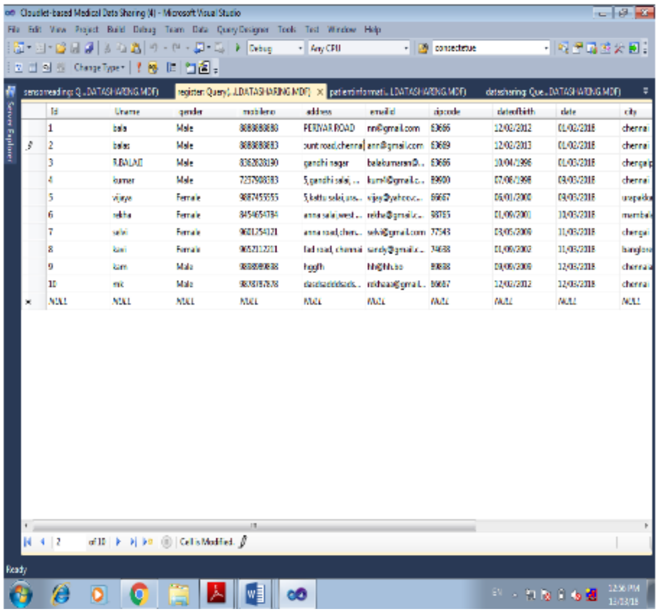
If the smart card of an authorized registered user is stolen/lost, the following steps are essential for obtaining a new smart card : Step 1. User keeps the same identity , but chooses a password then picks two random number , and computes pseudo-identity, pseudo password and then sends the registration request to the BRC securely.Step 2. On receiving pseudo-identity,pseudo password the BRC chooses a 160-bit random number , generates registration timestamp for User , computes an authenticator . The BRC then stores pseudo-identity , in CoT C's database in place of pseudo-identity , for further use corresponding to User . After that the BRC generates a new smart card new with the information and delivers it to User securely. Step 3. After receiving new smartcard , User computes a new register .User replaces a new register respectively. The smart card then contains the information For security reason, User discards A new register from Smartcard memory.

5.7 DYNAMIC WEARABLE SENSOR ADDITION PHASE

For deployment of a new wearable sensor node, say Sensor node in the existing network, the BRC does the following steps in offline mode: Step 1. The BRC picks a unique identity ,new Sensor node and a unique master key . After that the BRC calculates the secret key using its own secret key K and the corresponding secret credential Step 2. Finally, the BRC stores the information and into Sensor node' s memory before its deployment.

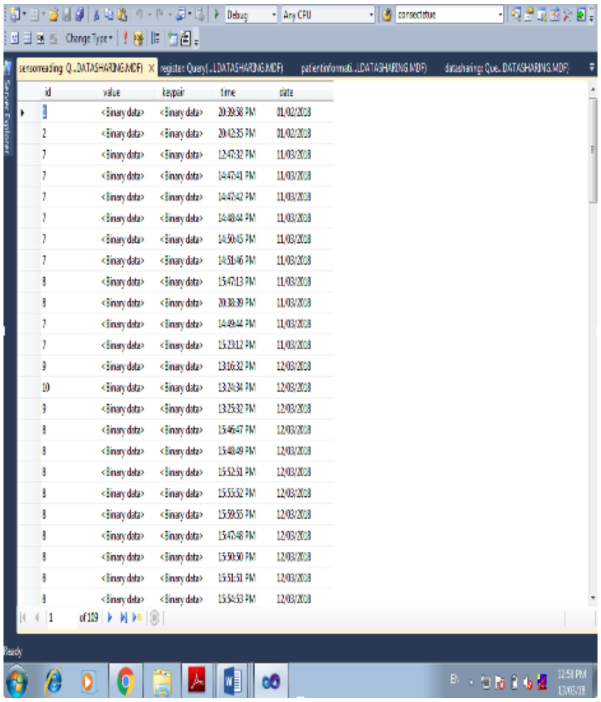
6. RESULT

6.1 REGISTER DATABASE


Cloudlet-based Medical Data Sharing (4) - Microsoft Visual Studio
File Edit View Project Build Debug Team Data Query Designer Tools Test Window Help
Debug
Any CPU
consectetue
Change Type
sensorreading: Q...DATASHARING.MDF)
register: Query(...DATASHARING.MDF)
patientinformati...DATASHARING.MDF)
datasharing: Que...DATASHARING.MDF)
Server Explorer
2 of 10
Cell is Modified.
Ready

Id	Uname	gender	mobileno	address	emailid	zipcode	dateofbirth	date	city
1	bala	Male	8888888880	PERIYAR ROAD	nn@gmail.com	63666	12/02/2012	01/02/2018	chennai
2	balas	Male	8888888883	ount road,chennai	ann@gmail.com	63669	12/02/2013	01/02/2018	chennai
3	R.BALAJI	Male	8362828190	gandhi nagar	balakumaran@...	63666	10/04/1996	01/03/2018	chengalp
4	kumar	Male	7237908383	5,gandhi salai, ...	kumi@gmail.c...	89900	07/06/1998	09/03/2018	chennai
5	vijaya	Female	9887455555	5,kattu salai,ara...	vijay@yahoo.c...	66667	06/01/2000	09/03/2018	urapakk
6	rekha	Female	8454654784	anna salai,west ...	rekha@gmail.c...	98765	01/06/2001	10/03/2018	mumbai
7	selvi	Female	9601754121	anna road,chen...	selvi@gmail.com	77543	03/05/2009	11/03/2018	chengai
8	kavi	Female	9652112211	fad road, chennai	sandy@gmail.c...	74688	01/06/2002	11/03/2018	banglore
9	kam	Male	9888989888	hggfh	hh@hh.bb	89888	09/06/2008	12/03/2018	chennai
10	mk	Male	9878787878	dasdsadddsads...	mdhaaa@gmail...	86687	12/02/2012	12/03/2018	chennai
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

6.2 SENSOR DATABASE



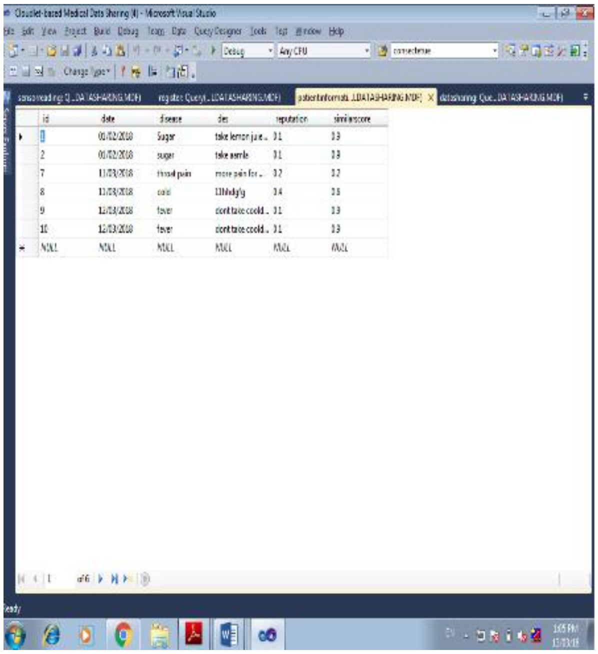
sensoreading: Q...DATASHARING.MDF) register: Query(...LDATASHARING.MDF) patientinformati...LDATASHARING.MDF) datasharing: Que...DATASHARING.MDF)

id	value	keypair	time	date
1	<Binary data>	<Binary data>	20:39:58 PM	01/02/2018
2	<Binary data>	<Binary data>	20:42:35 PM	01/02/2018
7	<Binary data>	<Binary data>	12:47:32 PM	11/03/2018
7	<Binary data>	<Binary data>	14:47:41 PM	11/03/2018
7	<Binary data>	<Binary data>	14:47:42 PM	11/03/2018
7	<Binary data>	<Binary data>	14:48:44 PM	11/03/2018
7	<Binary data>	<Binary data>	14:50:45 PM	11/03/2018
7	<Binary data>	<Binary data>	14:51:46 PM	11/03/2018
8	<Binary data>	<Binary data>	15:47:13 PM	11/03/2018
8	<Binary data>	<Binary data>	20:38:39 PM	11/03/2018
7	<Binary data>	<Binary data>	14:49:44 PM	11/03/2018
7	<Binary data>	<Binary data>	15:23:12 PM	11/03/2018
9	<Binary data>	<Binary data>	13:16:32 PM	12/03/2018
10	<Binary data>	<Binary data>	13:24:34 PM	12/03/2018
9	<Binary data>	<Binary data>	13:25:32 PM	12/03/2018
8	<Binary data>	<Binary data>	15:46:47 PM	12/03/2018
8	<Binary data>	<Binary data>	15:48:49 PM	12/03/2018
8	<Binary data>	<Binary data>	15:52:51 PM	12/03/2018
8	<Binary data>	<Binary data>	15:55:52 PM	12/03/2018
8	<Binary data>	<Binary data>	15:59:55 PM	12/03/2018
8	<Binary data>	<Binary data>	15:47:48 PM	12/03/2018
8	<Binary data>	<Binary data>	15:50:50 PM	12/03/2018
8	<Binary data>	<Binary data>	15:51:51 PM	12/03/2018
8	<Binary data>	<Binary data>	15:54:53 PM	12/03/2018

1 of 109

Ready

6.3 PATIENT MEDICAL INFORMATION DATABASE



Cloudlet-based Medical Data Sharing (4) - Microsoft Visual Studio

sensoreading: Q...DATASHARING.MDF) register: Query(...LDATASHARING.MDF) patientinformati...LDATASHARING.MDF) datasharing: Que...DATASHARING.MDF)

id	date	disease	des	reputation	similarscore
1	01/02/2018	Suger	take lemon jui...	0.1	0.3
2	01/02/2018	suger	take asmle	0.1	0.3
7	11/03/2018	throat pain	more pain for ...	0.2	0.2
8	11/03/2018	cold	11hhdg'g	0.4	0.5
9	12/03/2018	fever	dont take coold ...	0.1	0.3
10	12/03/2018	fever	dont take coold ...	0.1	0.3
NULL	NULL	NULL	NULL	NULL	NULL

1 of 6

Ready

7. CONCLUSION

In this paper, we checked the secure privacy protection problem and sharing of medical data in larger amounts in cloud. For the secure collection of data and low communication cost, we generated a system which will not allow users to transfer data to the remote cloud. But, it allow users to transmit data to a cloudlet, that is used to trigger the data sharing problem in the cloudlet. Initially, we can use wearable gadgets to collect users' information, and the transmission of users' data in order to ensure privacy of the users, we use NTRU mechanism. After the initial process,we use trust model to measure users' for the purpose of sharing information in the cloudlet and trust level to check whether to share data or not. Further, for securing of remote cloud data, we divided the data stored in the remote cloud and encrypt the data in several ways, it is not only used to protect information but to accelerate the transmission efficacy. Finally, we introduced collaborative IDS based on cloudlet mesh to secure the entire system. The proposed schemes are processed with simulations and experiments.

8. REFERENCES

[1] Deshpande, Vaibhav V., and Arvind R. Bhagat Patil. "Energy efficient clustering in wireless sensor network using a cluster of cluster heads." In 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-5. IEEE, 2013.

[2] Boulis, Athanassios, and Mani Srivastava.

"Node-level energy management for sensor networks in the presence of multiple applications." Wireless Networks 10, no. 6 (2004): 737-746.

[3] Jabbar, Sohail, Abid Ali Minhas, Anand Paul, and

Seungmin Rho. "Multilayer cluster designing algorithm for lifetime improvement of wireless sensor networks." The journal of Supercomputing

70, no. 1 (2014): 104-132.

[4] Jan, Hilal, Anand Paul, Abid Ali Minhas, Awais Ahmad,

Sohail Jabbar, and Mucheoul Kim. "Dependability and reliability analysis of intra cluster routing technique." Peer-to-Peer Networking and Applications 8, no. 5 (2015): 838-850.

[5] Ahmad, Awais, M. Mazhar Rathore, Anand Paul, and Bo-Wei Chen. "Data transmission scheme using mobile sink in static wireless sensor network." Journal of Sensors 2015 (2015).

[6] Ahmad, Awais, Sohail Jabbar, Anand Paul, and Seungmin Rho. "Mobility aware energy efficient congestion control in mobile wireless sensor network." International Journal of Distributed Sensor Networks 2014 (2014).

[7]Song, Min, and Bei He. "Capacity analysis for flat and clustered wireless sensor networks." In Wireless Algorithms, Systems and Applications, 2007. WASA 2007. International Conference on, pp. 249-253. IEEE, 2007.

[8] Iwata, Atsushi, Ching-Chuan Chiang, Guangyu Pei, Mario

Gerla, and Tsu-Wei Chen. "Scalable routing strategies for ad hoc wireless networks." IEEE journal on Selected Areas in Communications 17, no. 8 (1999): 1369-1379.

[9] Singh, Shio Kumar, M. P. Singh, and D. K. Singh.

"A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks." International Journal of Advanced Networking and Application (IJANA) 2, no. 02 (2010): 570-580.

[10] Yatika, Vikram nandal. "Increase throughput of a network through wireless sensor network." International Journal of Computer Science and Mobile Computing."

IJCSMC, vol. 3, Issue. 7, pg.310 317, 2014.

[11] Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and

Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." In System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on, pp. 10-pp. IEEE, 2000.

[12] Handy, M. J., Marc Haase, and Dirk Timmermann.

"Low energy adaptive clustering hierarchy with deterministic cluster-head selection." In Mobile and Wireless Communications Network, 2002. 4th International Workshop on, pp. 368-372. IEEE, 2002.