Cloud Centric Authentication for Wearable Health-care Monitoring System

Mr. Manjunath S,Mr. Govindraj T,Mr. Srinidhi Patwari

Associate Professor , UG Scholar,,UG Scholar,

ISE Department,

Global Academy of Technology, Bangalore, India

Abstract : ***Security and privacy are the major concerns in cloud computing as users have limited access on the stored data at the remote locations managed by different service providers. These become more challenging especially for the data generated from the wearable devices as it is highly sensitive and heterogeneous in nature. Most of the existing techniques reported in the literature are having high computation and communication costs and are vulnerable to various known attacks, which reduce their importance for applicability in real-world environment. Hence, in this project, we propose a new cloud-based user authentication scheme for secure authentication of medical data. After successful mutual authentication between a user and wearable sensor node, both establish a secret session key that is used for future secure communications. The extensively-used Real-Or-Random (ROR) model based formal security analysis and the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool based formal security verification shows that the proposed scheme provides the session-key security and protects active attacks. The proposed scheme is also informally analyzed to show its resilience against other known attacks. Moreover, we have done a detailed comparative analysis for the communication and computation costs along with security and functionality features which proves its efficiency in comparison to the other existing schemes of its category.***

I. INTRODUCTION

Cloud computing and Internet of Things (IoT) are two promising technologies which have gained a lot of attention in the recent years. Both technologies can be adopted to build important components of the future Internet. The Cloud IoT paradigm is considered as a paradigm where both cloud and IoT can be integrated together to provide better services including the health care applications using the wearable devices Nowadays, the wearable devices available in the market include smart watches and bracelets, wearable sleep aid devices, etc. Due to tremendous advancement in recent years in wearable techniques, these devices are broadly accepted in the market by the consumers. The data generated from the wearable devices has high sampling rate and hence, it needs to be stored and handled carefully at the cloud centric data server. A wearable sensor based medical system includes various flexible sensors worn on various parts of the body of a person (patient), 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.

The wearable sensors measure various physiological data including electrography, electrocardiogram, body temperature, heart rate, blood pressure, arterial oxygen saturation (SpO2),etc. The advances in wireless communication technology have conquered most of the temporal, geographical as well as organizational barriers to ease an entirely roaming way of transferring medical information and documentations to the concerned authorities. In this work, a scenario in the Cloud of Things Centric (CoTC) for a smart medical health-care system is considered, where a set of wearable sensor nodes are embedded.Gartner, Inc. forecasts that more than 8.4 billion connected IoT things (devices) will be used worldwide till 2020, which is higher than 31 percent than earlier years. It also forecasts that the number of connected IoT devices will reach 20.4 billion by the year 2020. 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 low-cost, it is the most suitable and cost effective solution to deal with big data produced by IoT devices.

II. LITERATURE SURVEY

[1]*Jubi Rana, Abhijeet Bajpayee, **"Healthcare Monitoring and Alerting System Using Cloud Computing",*** International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 3 Issue: 2015.A healthcare becomes a big issue due to lack of availability of expert doctors. Due to this issue there is a paradigm shift from need based health monitoring to preventive health monitoring service. Keeping in view this scenario we are proposing a health care system which will be integrated with cloud computing. That will make system capable of generating EMR i.e. Electronic Medical Records of patients which will play a beneficial role for patient's diagnostic and rapid improvement process as well as for medical practicing doctors who need vast medical cases for their own study purpose.

[2] A. Antony Viswasa Rani , E. Baburaj, ***"An efficient secure authentication on cloud based e-health care system in WBAN",*** Research Article - Biomedical Research Computational Life Sciences and Smarter Technological Advancement, 2016.In sensor networks, spoofing attack is trouble-free to initiate (i.e.) an attacker pretends to be someone else to gain access to restricted resources or to steal information. Most conventional security approaches used cryptographic authentication to prevent spoofing attacks. Due to their computational complexity these security approaches are not always desirable.This paper proposed an Integrated Secure Authentication (ISA) in e-health Care application using cloud environment to use spatial information of Received Signal Strength (RSS), a physical property associated with each node, that is difficult to modify and not based on cryptography.

[3] Prabal Verma1, Sandeep K. Sood, Sheetal Kalra, ***"Cloud-centric IoT based student healthcare monitoring framework",*** DOI 10.1007/s12652-017-0520-6, 2017.A cloud-centric IoT based smart student m-healthcare monitoring framework is proposed. This framework computes the student diseases severity by predicting the potential disease with its level by temporally mining the health measurements collected from medical and other IoT devices. In our case study, health dataset of 182 suspected students are simulated to generate relevant waterborne diseases cases. This data is further analyzed to validate our model by using k-cross validation approach. Pattern based diagnosis scheme is applied using various classification algorithms and then results are computed based on accuracy, sensitivity, specificity and response time.

[4] S.Challa, M.Wazid, A.K.Das, and M.K.Khan, ***"Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions"***, IEEE Consumer Electronics Magazine, vol. 7, no. 1,pp. 57–65, Jan 2018.Implantable medical devices (IMDs) are surgically embedded into a human body. These devices are increasingly being used for improving the quality of life of patients by treating various chronic ailments such as cardiac arrhythmia, diabetes, and Parkinson's disease. The received patient vitals are stored in a medical server through a controller node (CN). Due to the wireless communication of sensitive patient data over public channels, the information can be eavesdropped, modified, or deleted. Hence, security is a major concern while designing an authentication protocol in IMDs.[5] J.Wu, H.Li, S.Cheng, and Z.Lin, ***"The promising future of healthcare services: When big data analytics meets wearable technology"***, Information & Management, vol. 53, no. 8, pp. 1020–1033, 2016.

As policy-makers and business practitioners across the globe expend extraordinary effort toward the field of e-health, the thriving development of healthcare-wearable technology is creating great opportunities and posing a remarkable future for healthcare services. This paper employs a game theory model to investigate the dynamics of wearable device market. We extend the two-dimensional product differentiation model by incorporating consumer diversity, consumer density, and firms' big data analytics (BDA) investment strategy. Our model reveals that with differentiated consumer densities firms are more likely to engage in quality competition and the firm that invests in BDA can achieve higher profits. Furthermore, the overall quality of biomedical and healthcare services can be improved under various market conditions.

Our findings provide practical guidance to wearable device manufacturers on optimizing competition strategies and offer insights to social planners on potential policy-making to promote better healthcare services.

[6] ***"Information Matters. The Business of Data and the Internet of Things (IoT)",*** Accessed on 2017.

Finding "reliable" data about the installed base of Internet of Things (IoT) devices, market size and forecasts is not easy and can be expensive if you have to buy a commercial market report. However, there is quite a bit of free data out there which I have collated here. Creating IoT stats is notoriously difficult depending on accuracy of models, assumptions and definitions. Forecasts need to be treated very cautiously. However, by looking through a range of estimates from different providers it should be possible to get a rough idea of how the IoT market may look in the next few years. I have focused on providing links to the original sources where possible.

[7]M.D.Assuno, R.N.Calheiros, S.Bianchi, M.A.Netto, and R.Buyya, ***"Big Data computing and clouds: Trends and future directions"***, Journal of Parallel and Distributed Computing, vol. 79-80, pp. 3 – 15, 2015.This paper discusses approaches and environments for carryinganalytics on Clouds for Big Data applications. It revolves around four important areas of analytics and Big Data, namely (i) data management and supporting architectures; (ii) model development and scoring; (iii) visualisation and user interaction; and (iv) business models. Through a detailed survey, we identify possible gaps in technology and provide recommendations for the research community on future directions on Cloud-supported Big Data computing and analytics solutions.

III.EXISTING SYSTEM

Existing techniques reported in the literature are having high computation and communication costs and are vulnerable to various known attacks, which reduce their importance for applicability in real-world environment. Security is a major issue since, it is vulnerable to attacks.

DISADVANTAGES:

- Reduce their importance for applicability in real-world environment
- Less storage capacity and High-cost.
- It is the less suitable and cost effective solution to deal with big data.

IV. PROPOSED SYSTEM

We propose a new cloud based user authentication scheme for secure authentication of medical data. After successful mutual authentication between a user and wearable sensor node, both establish a secret session key that is used for future secure communications. The extensively-used Real-Or-Random (ROR) model based formal security analysis and the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool based formal security verification show that the proposed scheme provides the session-key security and protects active attacks.

ADVANTAGES:

- Provides a high security to the user data stored.
- Authentication is very strong that no attacks can be done.
- Provides High storage capacity.
- It is the More suitable and cost effective solution to deal with big data.

4.1 OBJECTIVES

- Here it is proposed a new cloud based user authentication scheme for secure authentication of medical data.
- Aftersuccessfulmutual authentication between a user and wearable sensor node, both establish a secret session key that is used for future secure communications.
- The scheme here proposed is also informally analyzed to show its resilience against other known attacks.
- Here all the users will be provided with high security authentication session key.
- Moreover, we have done a detailed comparative analysis for the communication and computation costs along with security and functionality features which proves its efficiency in comparison to the other existing schemes of its category.

V. SYSTEMARCHITECTURE

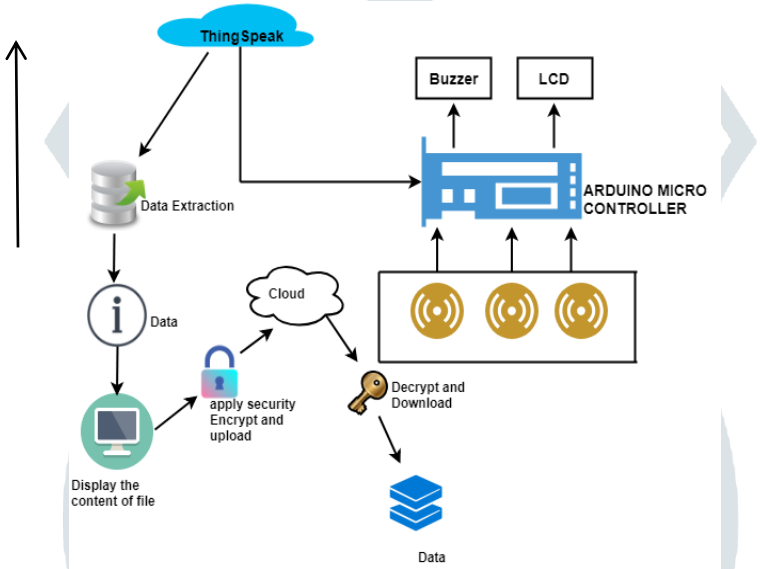

Fig 5.1: System Architecture

Here all the data generated from the Wearable devices from the various sources like Smart-phone, Local Health-care, Smart watches, etc. will be stored in the Health cloud data center with the help of the communication gateway/internet as shown in Fig 8.1.1.Now the data stored in the cloud need to be extracted by the Emergency Medical Aid, Medical Ad visor, Health-care Robots, Family Members, etc.The main aim here is to provide the security during the extraction of the data from the cloud towards the end users. Here we will make use of various **Encryption/Decryption Algorithms** for the enhancement of the security of the data.

5.1 Module:

1. Data Extraction:

   In this module taking the credential of thing speak in this one channel id , read key and write key applying in coding we are fetching the data from thing speak to java memory.

2. Analysis module:

   In this module already fetched thing speak values taking for the consideration we are giving condition. Based on conditions we displaying results.

VI. METHODLOGY

1. ECC Encryption/Decryption:

Several discretelogarithm-based protocols have been adapted to ellipticcurves, replacing the group with an elliptic curve:

- The Elliptic Curve Diffie–Hellman (ECDH) key agreement scheme is based on the Diffie–Hellman scheme,
- The Elliptic Curve Integrated Encryption Scheme (ECIES), also known as Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme,
- The Elliptic Curve Digital Signature Algorithm (ECDSA) is based on the Digital Signature Algorithm,
- The deformation scheme using Harrison's p-adic Manhattan metric,
- The Edwards-curve Digital Signature Algorithm (EdDSA) is based on Schnorr signature and uses twisted Edwards curves,
- The ECMQV key agreement scheme is based on the MQV key agreement scheme,At the RSA Conference 2005, the National Security Agency (NSA) announced Suite B which exclusively uses ECC for digital signature generation and key exchange. The suite is intended to protect both classified and unclassified national security systems and information. Recently, a large number of cryptographic primitives based on bi-linear mappings on various elliptic curve groups, such as the Weil and Tate pairings, have been introduced as shown in Fig 8.1.2. Schemes based on these primitives provide efficient identity-based encryption as well as pairing-based signatures, signcryption, key agreement, and proxy re-encryption.

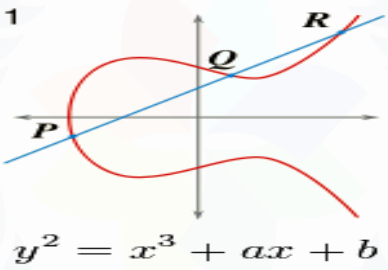

Fig 6.1: Eliptic Curve Cryptography

VII. CONCLUSION

A new user authentication scheme in which a legal user registered will be able to mutually authenticate with an accessible wearable sensor node.. At the end of successful mutual authentication between user and wearable sensor node, both establish a secret session key that is further used for future secure communications. The formal security using ROR model, informal security and formal security verification using ECC algorithm can give high confidence that several potential passive and active attacks performed by an adversary can be protected in the proposed scheme. In addition, a detailed comparative analysis for the communication and computation costs, and security and functionality features shows that there is a better trade-off among these components in the proposed scheme as compared to those for other schemes. The future work includes evaluating the proposed scheme in a real-world wearable devices deployment that will permit us to fine-tune the scheme, if necessary, to offer better performance as well as security.

REFERENCES

[1] Jubi Rana, Abhijeet Bajpayee, ”Healthcare Monitoring and Alerting System Using Cloud Computing”, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 3 Issue: 2015.

[2] A. Antony Viswasa Rani , E. Baburaj, “An efficient secure authentication on cloud based e-health care system in WBAN”, Research Article - Biomedical Research Computational Life Sciences and marter Technological Advancement, 2016..

[3] Prabal Verma1, Sandeep K. Sood, Sheetal Kalra, “Cloud-centric IoT based student healthcare monitoring framework”, DOI 10.1007/s12652-017-0520-6, 2017.

[4] S.Challa, M.Wazid, A.K.Das, and M.K.Khan, “Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions”, IEEE Consumer Electronics Magazine, vol. 7, no. 1,pp. 57–65, Jan 2018.

[5] Wu, H.Li, S.Cheng, and Z.Lin, "The promising future of healthcareservices: When big data analytics meets wearable technology", Information & Management, vol. 53, no. 8, pp. 1020–1033, 2016.Information Matters. The Business of Data and the Internet of Things (IoT)", http://informationmatters.net/internet-of-things-statistics/, Accessed on August 2017.

[6] M.D.Assuno, R.N.Calheiros, S.Bianchi, M.A.Netto, and R.Buyya, "Big Data computing and clouds: Trends and future directions", Journal of Parallel and Distributed Computing, vol. 79-80, pp. 3 – 15, 2015.

[7] R.Alguliyev and Y.Imamverdiyev, "Big Data: Big Promises for Information Security", in IEEE 8th International Conference on Applicationof Information and Communication Technologies (AICT), Astana, Kazakhstan,2014, pp. 1–4.