International Journal of Global Engineering (IJGE) E-ISSN: 2456-3099

VOL 2 ISSUE 3 (2018) PAGES 49 - 54

Received: 20/02/2018. Published: 22/03/2018

A ROBUST PRIVACY PRESERVING FOR E-HEALTH SYSTEMS THROUGH THREE FACTOR KEY AGREEMENT

D.E.Gowthami[1], P.Jayashree[2], S.Meena[3], A.S.Vibith[4]
Department of Computer Science and Engineering
Students[1,2,3], Assistant Professor[4]
Kingston Engineering College, Vellore, India.

ABSTRACT:

In this share shock and phonegregation world, the electronic healthcare (e-health) system has been evolved into a patient-oriented service with smaller and smarter wireless devices. As these convenient smart devices come with small computational capacity and memory size, protection of the user's massive private data becomes difficult. The works done to ensure privacy of the e-health system using the biometric authentication is also vulnerable. In this study, we use a graphical password as an additional factor in the authentication process which will overcome the vulnerability and provide the most secured authentication.

1. INTRODUCTION

E-HealthCare is an informative and interactive method that both patients and health care professionals can come together and share information with others in the profession from around the world. Gone are the days where people generally go to a doctor or a provider when they are sick; which was more episodic. Today, we see healthcare being delivered as a subscription where providers are actively involved in your care and reach out to you for an intervention instead of the other way round.

This will be made possible with wearables, as providers will have access to real-time data. With tremendous scope for innovation, the possibilities for ensuring better healthcare outcomes are enormous but the patient's privacy is susceptible to several attacks as they are transmitted over unsecured public networks. The least expected thing happens, unauthorized adversaries may get access to the patient's current health condition, medical history and other binding information like mobile phone number and credit card number. The patient will suffer much more than the illness itself. To deal with this situation, several key agreement and authentication mechanisms were implemented but then we weren't able to provide a robust security mechanism. This led to the use of biometrics as a factor for authentication purpose. But due to misuse of biometric image, time complexity and in order to make a human friendly authentication system we introduced graphical password as an authentication factor in e-health systems so that it would be much easier when all classes of people make use of this e-health systems.

Received: 20/02/2018. Published: 22/03/2018

II. EXISTING SYSTEM

The electronic healthcare (e-health) system has been evolved into a patient-oriented service with smaller and smarter wireless devices. As these convenient smart devices have limited computational capacity and memory size, it is harder to protect the user's massive private data in the e-health system. In the existing system, biometric authentication system is used in order to secure the user's private data. The Biometric Features is basically used to identify the individuals Face, Fingerprint, Handprint, Voice etc. If we consider the Handprint, it will also be unique for each and every person. In the existing system handprint/fingerprint is used as an authentication factor using various hash functions, bio hash functions and dynamic mechanisms in order to provide security to the user's private data.

DISADVANTAGES OF EXISTING SYSTEM:

- But even the fingerprint gets similar between people at some cases.
- As this is a web application, an external device is needed in order to scan the fingerprints.
- Misuse of fingerprints when it is used by saving in our systems or devices.
- Time complexity as it has to calculate hash functions, bio functions and dynamic mechanism.

III.LITERERATURE SURVEY

[1]This paper proposes a polynomial-time algorithm for energy-efficient dynamic packet downloading from medical cloud storage to medical Internet-of-Things (IoT) devices. The medical cloud can distribute its own medical data to medical IoT devices via access points. Therefore, network disconnection can happen between the medical cloud and medical IoT devices when power/energy management in each access point is not efficient. Therefore, this paper proposes a dynamic energy-efficient algorithm, which computes the amount of power allocation in each access point based on the buffer backlog size and channel states under the consideration of buffer stability. With the proposed adaptive algorithm, each access point calibrates its own parameters for more adaptive power/energy management.

[2]Over the last few years various AAL systems, mostly based on Wireless Body Area Network technologies, have been proposed to improve the quality of life of elderly people. Since the information transmitted in AAL systems is very personal, the security and privacy of such data are becoming important issues that must be dealt with. Next we propose an efficient authentication protocol for the AAL system and describe how it meets various security requirements. Finally we compare the performance of the proposed authentication protocol with two other recent authentication protocols and demonstrate its superior efficiency.

[3]This paper proposes a chaotic map-based key agreement protocol without using smart cards. They claimed that the protocol is secure against password-guessing attacks. However, we show that Gong et al.'s protocol is vulnerable to partition attacks, whereby the adversary can guess the correct password off-line. We also demonstrate that the protocol suffers from a stolen-verifier attack along with password change pitfalls. Thereafter, we proposed an chaotic map-based key agreement protocol without using smart cards to conquer the mentioned weaknesses. The security analysis of the proposed protocol shows that it is suitable for the applications with higher security requirement.

IV.PROPOSED SYSTEM

In our proposed system, we have included graphical password as an additional factor for authentication purpose. At first the user registers his personal details along with a graphical password. Whenever the user wants to send a query to the doctor he logins using his graphical password for authentication purpose and then the graphical password of the user is sent to e-doctor as a mail from the server mail. In order to decrypt the queries sent by the user/the patient, the doctor has to enter or reproduce the graphical password of the user which was sent as a mail by the server to the doctor's mail id. Thus this will overcome all the vulnerabilities encountered in the existing system.

ADVANTAGES:

- Human friendly passwords.
- It serves as conflicting requirements i.e easy to remember and hard to guess.
- Dictionary attacks and brute force search are infeasible.
- Reduced time complexity and design complexity.

V. ARCHITECTURE

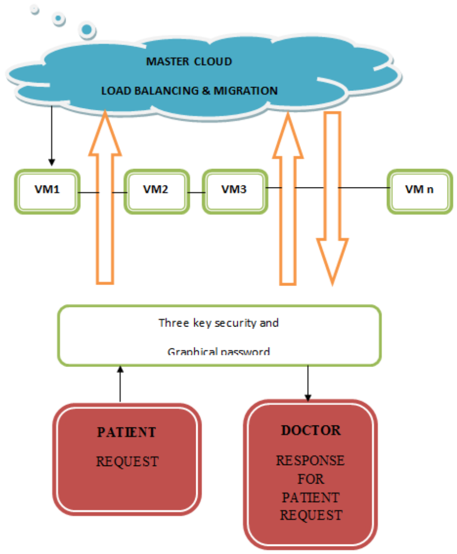

Figure: Architecture Diagram

VI. ALGORITHM

GRAPHICAL AUTHENTICATION

A graphical password is an authentication system that works by having an user select from images in a specific order presented in a graphical user interface (GUI).

```
<%

String x1,x2,y1,y2;

String xx1,xx2,yy1,yy2;

String uid =  request.getParameter("uid");

x1=request.getParameter("x1");

x2=request.getParameter("x2");

y1=request.getParameter("y1");

y2=request.getParameter("y2");

xx1=request.getParameter("xx1");

xx2=request.getParameter("xx2");

yy1=request.getParameter("yy1");

yy2=request.getParameter("yy2");

System.out.println(x1+" "+xx1+" "+y1+" "+yy1+" "+x2+" "+xx2+" "+y2+" "+yy2);

if(x1.equals(xx1)&&x2.equals(xx2)&&y1.equals(yy1)&&y2.equals(yy2))
{
session.setAttribute("uid", uid);

out.println("<script>"+"alert('Co-Ordinates Matched..')"+"</script>");

RequestDispatcher rd=request.getRequestDispatcher("PatientsQuery.jsp");

rd.include(request, response);
}
```

Received: 20/02/2018. Published: 22/03/2018

```
else
{
out.println("<script>"+"alert('Sorry Please Try Again')"+"</script>");

RequestDispatcher rd=request.getRequestDispatcher("PatientsQuery1.jsp");

rd.include(request, response);
}
%>
```

CONCLUSION

In this work, we have proposed graphical password as an authentication factor to provide enhanced security to the e-health systems than the previous system. The traditional biometric authentication is replaced by a graphical password authentication to provide intractability so that the user anonymity can be fully preserved. In addition our methodology or technique serves as a human friendly password making all classes of people to access and make use of e-health systems for continuous monitoring and maintaining of their health system. Therefore the proposed scheme meets the security needs of e-health systems successfully.

REFERENCES

1.J.Kim, “Enrgy-efficient Dynamic Packet Downloading for Medical IoT Platforms,”IEEE Transactions on Industrial Informatics, vol 11,pp.1653-1659, Dec 2015.

2.D.B.He andS.Zeadally , Äuthentication Protocol for an Ambient Assissted Living System,”IEEE Communications Magazine, vol.53,pp.71-77, jan 2015.

3. E.J. Yoon and K.Y. Yoo, “Robust biometrics-based multi-server authentication with key agreement scvheme for smart cards on elliptic curve cryptosystem,”Journal of Supercomputing,vol.63,pp.235-25jan 2013.

4.M.S Fransh and M.A. Attari, “Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing,”NonlinearDyanmics,vol.76,pp.1203-1213,apr 2014.

5.A.K. Das,P.Sharma,S.chatterjee,and J.K.sing,”A dynamic password-based user authentication scheme for hierarchical wireless sensor networks,”Journal of Network and Computer Applications, vol.35,pp.1646-1656,sep 2012.

Received: 20/02/2018. Published: 22/03/2018

6.X.X.Li,W.D.Qiu,D.Zheng K.F.Chen,and J.H.Li,”Anonymity Enhancement on robust and efficient password-authenticated key agreement using smart cards,ÏEEE Transcations on Industrial Electronics,vol.57,pp.793-800,feb 2010.

7.J.L.Tsai,N.W.Lo,andT.C.Wu,”Novel Anonymous Authentication Scheme using smart cards,ÏEE Transactions on Industrial Informatics,vol.9,pp.2004-2013,nov2013.