A Novel Authentication Framework for IoT-Based Healthcare Systems

Anitha Rani S, Dr. K. Ramesh Kumar*

Research Scholar, Department of Computer Science, Loyola College (Autonomous), Chennai, Tamil Nadu, India.
Associate Professor, Department of Computer Science, Loyola College (Autonomous), Chennai, Tamil Nadu, India.

ABSTRACT

The Internet of Things (IoT), interconnection of huge number of everyday objects, is the future of the scientific world. The increasing amounts of devices with Wi-Fi capabilities allow them to send and receive data. Now-a-days smart phone is with everybody and its usage is sky-rocketing. This gives way to connect anything that can be connected, will be connected and secure sharing of information critical. In this paper, the existing works are analyzed and new architecture for Smart healthcare system is proposed. A neoteric authentication scheme that supplements the security of the smart healthcare system is also proposed.

KEYWORDS: IoT, Architecture, Enhancing Authentication, Smart Healthcare System, Security, IoT devices.

INTRODUCTION

The Internet of Things spins around increased machine-to-machine communication today. It is built on cloud computing and interconnection of data-accumulating sensors. It is purely mobile, virtual, and instantaneous connection. In current scenario, it is going to make everything in our lives from streetlights to seaports "smart." It will involve and do wonders in many areas such as assisted-living, healthcare, enhanced learning, computerization and engineering, logistics, process administration and smart conveyance. US National Intelligence Council named "Internet of Things" as the ''Disruptive Civil Technologies" in its report [1]. A UN Report predicts a new age of ubiquity where people become the minority as producers and receivers of traffic and changes carried by the Internet [2]. This new scenario enables the connectivity from anywhere and anytime with any communication device. It is highly influential on several aspects of everyday-life. Though, many researches are going on in this field it is still in infancy and has many issues and challenges to be resolved. Apart from heterogeneity, scalability, connectivity and lot many other issues, security issues prove to be major contributors in impinging the development IoT and have to be dealt with effectively to make IoT a fruitful reality. One such prominent security issue is authentication of devices participating in IoT among other security issues such confidentiality, integrity etc. which is the main focus of this paper.

Section II a briefs on the necessary background on Internet of Things. Section III elaborates the security issues in IoT. Section III presents some of the authentication schemes available in the literature. The proposed architecture for an IoT enabled healthcare system and the workflow of the system, are presented in Section IV. The proposed authentication technique that could be integrated with the proposed IoT enabled healthcare system is discussed in Section V and the conclusion is presented in Section VI.

BACKGROUND

Research in Mobile Computing (MC), Pervasive Computing (PC) and Wireless Sensor Networks (WSN), Mobile ad-hoc Network (MANET) are in full swing for more than a decade. Internet of Things which is a combination of these has emerged recently and has gained much popularity. Gartner defines Internet of Things as the network of physical objects with embedded technology, capable of communicating and sensing or interacting with their internal states or the external environment [3]. With IoT, smart objects or people can interrelate and interconnect among themselves with the environment.

It is stated by Cisco that the number of devices connected to the Internet will overtake the human total population and there will be nearly 50 billion devices connected to the internet by 2020 [18]. As more and more gadgets emerge, these tend to participate in an IoT environment which in turn leads to the generation and exchange of enormous amount of data. Hence, provisioning security in an IoT environment is more complex than imagined. To guarantee security in IoT, properties such as confidentiality, integrity, authentication, privacy, authorization and availability must be assured. On one hand ensuring ample security to the data is a herculean task in such a scenario while on the other hand the source of data themselves need to be authenticated for the user of the data to rely on the data for further action.

Cryptographic mechanisms can be used as a healthy way of safeguarding communication over the Internet of Things mainly for embedded systems, where security burdens are rising these mechanisms can be used to defend against counterfeiting, firmware tampering and illegal access. However, source authentication is the process of recognizing users, computers, devices and machines in the IoT environment and this actually rely on usernames and passwords. To be secure enough, the username password scheme requires frequent changing and do not work with unattended devices in IoT. Authentication of IoT devices in a healthcare domain is all the more important, as the data source must be trustworthy to provide proper treatment to the patient. Hence, in this paper we propose a novel device authentication technique based on device registration.

REVIEW OF LITERATURE

Eleonora Borgia offered vital features, the driving technologies of IoT, focused on the research problems and open disputes of it [3]. The author drew an image of the IoT paradigm, and the recent IoT research accomplishments. The author has highlighted the contributions of recent research. Moreover, the author emphasized the standardization activities to avoid excessive fragmentation and discussed the key tactical business priorities providing an overview of the key sectors. Andrew et al., presented the researches in IoT, categorized current trends and the challenges of IoT diffusion [5]. They also listed IoT open research questions and future directions to support scholars. They grouped the IoT challenges based on technology, application and business models. Hardware, software and architecture oriented issues were also highlighted.

S. Madakam et al., presented a review of Internet of Things by analyzing various white papers and online databases [6]. They outlined the IoT overview, architecture and technology used in it.
John Pescatore presented security concerns of IoT in the SANS analyst report [7]. This report emphasized on securing IoT, which would increase the visibility for common customer. The author pointed out that Internet of Things too, have same kind of security issues like other technologies. Jorge Granjal et al. studied the protocols and mechanisms to defend communications in IoT [8]. They examined the already available approaches for security and outlined new trials and policies for future. Communication protocols according to the architecture of IoT such as 6LoWPAN, ROLL, CoAP and IEEE 802.15.4 were listed and their main characteristics were explained.

J. Sathish Kumar et al. introduced IoT as a unified system [9]. The authors raised their concern over individual privacy and access of personal information related to devices. They summarized the security threats based on Front-end Sensors and Equipment, network and Back-end of it systems. Privacy in the device, in storage during communication and at processing of IoT data and user were addressed. Md. Mahmud Hossain et al. articulated their concern over on the security problems [10]. They pointed out that though there is extensive distribution of IoT devices, there are still many open problems in the IoT environment. They explained the components of the IoT network and conducted a deep analysis of the security issues based on hardware, software and network. Factors that were required while providing security solution to the IoT devices based on information security, access level security and functional security were also discussed. IoT attack surfaces, forensics, security issues, threat models, requirements and challenges were detailed by the authors. They also highlighted IoT security and privacy.

Qi Jing et al., published a survey on IoT security architecture and security issues concentrated on the three layers such as perception, transportation and application layers [11]. Security concerns of each layer were studied and classic solutions were proposed for them. The features of diverse solutions and the technology involved in them were elaborated. The security issues of IoT were compared with traditional network security issues. The authors expressed their concern on the unsafe situation of the IoT environment with inadequate resources and a reduced amount of network guards. So they insisted on the requirement of new lightweight solutions for IoT security.

J. H. Ziegeldorf et al., worked on the privacy disputes of IoT [12]. They studied the privacy consequences and threats. They elaborated on the privacy issue with an IoT reference model for precise objects and current privacy legislation. The impact of privacy threats in seven categories such as identification, tracking, profiling, linkage, Interaction and presentation, lifecycle transitions and inventory attacks were also presented by the authors. S. L. Keoh et al., elaborated the efforts of Internet Engineering Task Force (IETF) to regulate security solutions for IoT [13]. In particular, they explored the features of Standard security protocols with the Constrained Application Protocol (CoAP) which was specifically tailored for IoT devices and underscored the use of Datagram Transport Layer Security (DTLS) as a channel for security under CoAP.

Security issues and challenges were discussed by Farooq et al. They proposed an architecture with reference to confidentiality and privacy of the user [14]. They gave high precedence to the security of IoT and defined

security infrastructure protocols that could address the challenges of scalability, availability and security of IoT. The authors pointed out the research achievements in IoT security and insisted the need for the expansion of these security solutions to satisfy the futuristic data-hungry devices. S. R. Moosavi et al., designed a secure mutual authentication scheme for RFID implant system [15]. They used elliptic curve cryptography and the D-Quark lightweight hash design in their proposed scheme. The small key sizes and the efficiency of the elliptic curve-based cryptosystems made them to select this algorithm for their computations. Moreover, they claimed that the D-Quark lightweight hash design was best suited for resource limited pervasive devices, and was cost effective, and offered better performance. They projected that their authentication scheme was secure against the pertinent threat models and offered a higher security level. They also proved that their system gave 48% less communication overhead and 24 % less total memory than the previous systems.

Manoj Kumar presented already proposed RFID authentication schemes [16]. He discussed the security necessities of RFID authentication structures, and offered a review of ECC-based RFID authentication schemes based on performance and security, mutual authentication, confidentiality and forward security. He also stated that the heavyweight schemes involved very complex operations such as public-key encryption and digital signature. But the middleweight schemes used both elliptic curve operations and hash functions. Usha devi et al., proposed a new authentication scheme based on two different approaches [17]. When an IoT device tried to connect from the same area of the network, the basic information of the device was collected and stored in a database for further references. These details were updated frequently and maintained in a DBMS which resides in the internet. The existing user was provided authentication using his login id and a hashing password or with the MAC passwords. Their method was proved for resistance against node compromise, communication overhead, computation overhead, robustness to packet loss and message entropy.

OBJECTIVE OF THE PROPOSED WORK

Though IoT is used in all scenarios, healthcare system gains more attention because it concerns life. In healthcare industry IoT increases efficiency, reduces costs and lays the focus on better patient care. As the wide intention is to create a patient-centered healthcare, IoT helps to monitor the patient continuously both in the hospital environment and remotely. With the intelligent system of IoT, one can obtain an exceptional level of real-time, life-critical data. The data accumulated and saved is analyzed by the intelligent system to drive efficacy, maintain compliance, and help the healthcare people to advance research, management and care.

In this scenario, authentication of IoT devices is a core issue. As there are multitude of devices deployed to accumulate the healthcare data of a patient, device authentication will play a crucial role. It is the need of the hour to propose an IoT enabled architecture with enhanced authentication for healthcare environment. Hence, this paper aims to suggest a new authentication scheme for IoT enabled healthcare devices.

PROPOSED ARCHITECTURE FOR IOT ENABLED HEALTHCARE SYSTEM

The amount and the variety of user and medical devices connected to the IoT healthcare system is on the rise. There is a drastic development in connecting everything in a patient's room including lights, air-conditioner, patients' bed and so on. The physical and cyber world connectivity of the IoT enabled healthcare system are in three different layers. They are: (i) Perception Layer (ii) Network Layer and (iii) Application Layer.

Each layer has different interacting technologies, protocols, purposes and functions. They are explained below:

a. **Perception Layer:** The devices deployed in a room of the healthcare system, sense the physical environment and collect the real time data. RFID tags, sensors and IPV6 are used to identify the medical devices along with their Electronic Product Codes (EPC). ZigBee, Bluetooth, and 3G / 4G technologies are used for communication.
b. **Network Layer:** This layer handles the communication of collected data to the Cloud Central Servers (CCS), Gateway Servers (GS) and different applications. Wired or wireless are used to access the network through gateways and addressing and routing of the data packets are handled by the routing protocols such as LEACH and RPL.
c. **Application Layer:** The collected data are managed by this layer and processed information is sent to the applications. Identification and management of user devices are the responsibilities of this layer. Moreover, collection and filtering of the data, data analysis and communication of derived information to application are also managed by this layer.

The proposed architectural design based on these layers is presented in Fig. 1.

Fig. 1. Architecture of the IoT enabled Healthcare System

WORK FLOW OF THE PROPOSED SMART HEALTH CARE SYSTEM

The proposed IoT enabled healthcare system setup is as follows. Every device in the proposed system is considered as individual nodes and they are interconnected by direct Ethernet or Wi-Fi connectivity, Near Field Communication, Bluetooth, ZigBee or other mesh radio networks technologies. Two types of users namely Privileged Users and Ordinary Users can only read the data collected by these nodes. The doctors, nurses and the close relatives of the patients come under the first group namely Privileged Users. The other medical information users such as medical researchers, medical insurance companies and the drug designers are treated as Ordinary Users. The details of the patients' relatives are collected at the time of admission of the patient to the hospital. The necessary information related to the physical condition of the patient is sent to them as SMS along with the details of the doctor. All the people other than the visitors of the patient are authenticated by the RFID tag.

Two kinds of devices are involved in the system namely User Device (ud) and Medical Devices (md). User Device (ud) may be a desktop, laptop, tablet or mobile phone using which the users access the medical information of the patient from the Medical Devices (md) in the patients' room which record various health parameters of the patient and store them in the cloud storage. When a user wishes to access the information recorded by any of the medical device, the user has to undergo an authentication process. The user devices as well as the medical devices participate in the authentication process using their IP addresses (IPudi, IPmdj) where i and j are the user device number and medical device number respectively.

Continuous medical information and streaming data of the patients are stored in Cloud Central Repository (CCR) and their meta-data such as CCR details, are stored in Gateway Server (GS). The users of the system interact with the Gateway Server through their user devices and access the necessary data by providing their authentication information. Moreover, streaming data from all the deployed devices are aggregated in a Cloud Central Repository (CCR) for future reference. The device authentication details are also maintained in this Cloud Central Repository.

PROPOSED AUTHENTICATION SCHEME

Since, the applications of IoT is enormous and the number of medical and user devices connected with the worldwide web is keeping on growing, prevention of unauthorized access to IoT data is essential. Since sharing the medical facts of a patient is unethical, the data collected from such environment should be maintained securely. To enhance the security of IoT healthcare data, the user devices which take part in this process must be authenticated. It is important that the identity of the user and the devices have to be managed properly.

Hence, authentication of devices and authorization of access to the healthcare data are key challenges in IoT enabled healthcare system. Normally, authentication and access authorization to IoT user devices use single password mechanism. But such mechanisms are often vulnerable to attacks. Even though this single password authentication technique is easy to remember, it paves ways for the intruders to break it. If anybody gets the password, he / she may try to access the healthcare data of a patient intentionally. And also one may try to re-program the medical devices which may collapse the entire system.

Based on the literature, we propose a novel authentication scheme for user devices. The User Device Authentication Procedure is presented in Fig. 2.

Step 1: The user requests data from a medical device through his user device.
Step 2: The medical device forwards the user request to the GS
Step 3: GS sends an authentication request to the CCR.
Step 4: CCR checks whether IP_{ud} is present.
Step 5: If IP_{ud} is not present, the user is a new user. So Go to Registration Phase
Else CCR challenges the device by asking its EPC_{ud} and password
Step 6: Device responds by sending its EPC_{ud} and password
Step 7: CCR checks the EPC_{ud} corresponding to the IP_{ud} stored in the User Device Registration Table.
Step 8: IF EPC_{ud} matches, the CCR checks the Access Control Table for providing access to the medical device.
Step 9: If access is allowed,
CCR provides a key generate response to the GS.
The GS issues the session key to the user.
Else the CCR sends an authentication failed message to the GS which is forwarded to the user.

Fig. 2. User Device Authentication Procedure

SCOPE OF IMPLEMENTATION OF THE PROPOSED AUTHENTICATION CHEME

There are three steps in the proposed authentication namely registration, authentication of the user device and authorization to a user device. They come under the umbrella of the identity management.

Registration Phase: Anybody who tries to access the IoT data has to register their user device (ud) before accessing the data. The IPv6 address of the device is collected along with its Electronic Product Code (EPC) in the Registration Phase. When registering the user device, the user selects a password. It is immediately encrypted and the encrypted password is stored in the User Device Registration Table in the CCR along with the password selected by the user.

The procedure of the Registration Phase is presented in the Fig. 3.

Step 1: CCR asks for IP address of the User Device (IP_{ud})
Step 2: User Device responds with the IP_{ud}
Step 3: CCR asks to select a password by following Rules_Pass_Sel()
Step 4: Pass(ud) is encrypted using encry(pass(ud)) and saved as pass(ud1)
Step 5: CCR asks the EPC of the device
Step 6: CCR sends the IP_d, EPC(ud) and Pass(ud1) to the GS
Step 7: GS sends the Ip_{ud}, Pass(ud1) and EPC(ud) to the CCR
Step 8: CCR saves all the information for further references

Fig. 3. User Device Registration Procedure

In the above mentioned procedure in Fig. 6, two functions are employed namely Rules_Pass_Sel() and encry(pass(d)). The Rules_Pass_Sel() displays the rules for selecting a password. The function encry(pass(d)) uses the ASCII code of the password and ceaser cipher to encrypt and encrypted user password is saved in the CCR. Pseudocode for function Rules_Pass_Sel() is presented in Fig. 4.

```
function Rules_Pass_Sel()
{     get pass(ud)
  if len(pass(ud)) < 8 then
       print 'Password must have at least eight characters long' end if
  for i← 1 to len (pass(ud))
    if char(pass(d)) not having any digit then
       print 'Password must have at least one digit' end if
  if char(pass(ud)) not having special characters <., -, _> then
       print 'Password must have at least one special character' end if
  if len(char(pass(ud))) <5 then
       print 'Password must have at least five character' end if
  end for
  pass(ud1)← encry(pass(ud))
  store pass(ud) and pass(ud1) in the CCR   }
```

Fig. 4. Function Rules_Pass_Sel()

Sample content of the User Device Registration Table is shown in Table 1.

Table 1. User Device Registration Table

IP Address	EP Code	Encrypted Password
IP_{ud1}	EPC_{ud1}	E(Pass(ud1))
IP_{ud2}	EPC_{ud2}	E(Pass(ud2))
..	..	..
..	..	..
IP_{udn}	EPC_{udn}	E(Pass(udn))

Authentication Phase: The users of the IoT enabled healthcare system are the doctors, ward nurses, patient relatives, medical insurance companies, medical researchers and the drug designers. They can only read the medical information available in CCR and they are restricted from performing any modification in the CCR. The User Access Control Matrix is presented in Table 2. In Table 2, '1' represents 'access allowed' and '0' represents 'access denied'. For example the row1 of Table 2 suggests that User Device IPud1 has read access to the data recorded by Medical Device IPmd1, IPmd2 and IPmdn and no such access is provided to the IPmd3.

During Authentication Phase, the user requests data from medical device through his user devices such as laptop, PDA, Tablet, Mobile phones and Desktop etc. When any medical device receives such request from the user devices, it immediately forwards the user request to its Gateway Server. The Gateway Server sends an authentication request containing <IDud, IPud, IPmd,> to the CCR to check whether the user can access the data corresponding to the medical device. CCR checks whether IPud is present in the User Device Registration

Table. If IPud is not present in the User Device Registration Table, then the request is from a new user. So the user has to undergo the Registration Phase by registering his IPud , EPCud and selecting a password for his device.

Table 2. User Access Control Matrix

	IP_{md1}	IP_{md2}	IP_{md3}	..	..	..	IP_{mdn}
IP_{ud1}	1	1	0	..	..	..	1
IP_{ud2}	0	0	1	..	..	..	0
IP_{ud3}	1	1	0	..	..	..	0
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
IP_{udn}	0	1	0	..	..	..	1

If requested user is an already registered user, CCR challenges the device by asking its EPCud and password. While the User Device responds to this challenge, the CCR checks the EPCud corresponding to the IPud stored in the User Registration Table. If the CCR finds the match in EPCud, then, it checks the Access Control Table to ensure whether the user device (IPud) can access the data corresponding to the medical device (IPmd).

Authorization Phase: If access is allowed, CCR provides a key generate response to the GS. After receiving such key generate response from the CCR, the Gateway Server responds by issuing the session key to the user for accessing the data corresponding to the device. If access is not allowed for the particular medical device to this user in the Access Control Table then, CCR sends an authentication failed message to the GS which is in turn forwarded to the user. Once the user device receives a session key from the GS, then it has access to the data generated by that particular medical device till the session key expires.

CONCLUSION

In this paper, an architecture that could enhance the authentication of devices in the IoT enabled smart healthcare system is presented. The mechanism proposed to authenticate each IoT device is expected to assure secure accessibility of medical data and is deployable, and applicable to the IoT devices.

REFERENCES

1. National Intelligence Council, Disruptive Civil Technologies - Six Technologies with Potential Impacts on US Interests Out to 2025-Conference Report CR 2008-07, April 2008, Online: www.dni.gov/nic/NIC_home.html.
2. Maarten Botterman, “Internet of Things: an early reality of the Future Internet”, European Commission, Information Society and Media Directorate, 2009.
3. Gartner-IT-Glossary, available at: http://www.gartner.com/it-glossary/internet-of-things/
4. Eleonora Borgia, "The Internet of Things vision: Key features, applications and open issues", Computer Communications Vol. 54, 2014, pp.1-31.
5. Andrew Whitmore, Anurag Agarwal, and Li Da Xu. "The Internet of Things-A survey of topics and trends", Information Systems Frontiers Vol. 17, Issue. 2, 2015, pp. 261-274.
6. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, "Internet of Things (IoT): A Literature Review", Journal of Computer and Communications, Vol. 3, Issue. 05, 2015, pp. 164-173.
7. John Pescatore, and G. Shpantzer, "Securing the Internet of Things Survey" , SANS Institute, 2014, pp. 1-22.
8. Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues", Communications Surveys & Tutorials, IEEE, Vol. 17, Issue 3, 2015, pp. 1294-1312.
9. J. Sathish Kumar and Dhiren R. Patel, "A survey on Internet of Things: security and privacy issues", International Journal of Computer Applications, Vol. 90, Issue. 11, 2014, pp. 20-26.
10. Md Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", Services, IEEE World Congress on. IEEE, 2015, pp. 1-8.
11. Jing, Qi, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu, "Security of the internet of things: Perspectives and challenges." ,Wireless Networks, Vol. 20, Issue. 8, 2014, pp. 2481-2501.
12. Jan Henrik Ziegeldorf, Oscar García Morchon, and Klaus Wehrle, "Privacy in the Internet of Things: threats and challenges", Security and Communication Networks, Vol. 7, Issue. 12, 2014, pp. 2728-2742.
13. Sye Loong Keoh, Sahoo Subhendu Kumar, and Hannes Tschofenig, "Securing the internet of things: A standardization perspective", Internet of Things Journal, IEEE, Vol. 1, N0. 3, 2014, pp. 265-275.
14. M. U. Farooq, Muhammad Waseem, Anjum Khairi and Sadia Mazhar "A critical analysis on the security concerns of internet of things (IoT)", International Journal of Computer Applications, Vol. 111, No. 7, 2015, pp. 1-6.
15. Sanaz Rahimi Moosavi, Ethiopia Nigussie, Seppo Virtanen and Jouni Isoaho, “An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems”, Procedia Computer Science (Elsevier), Vol. 32, 2014, pp. 198 – 206
16. Manoj Kumar S, “An Analysis of Authentication Schemes for Internet of Things”, International Journal of Engineering Sciences & Research Technology, Vol. 4, Issue 6, 2015, pp. 978 – 984.
17. G. Usha Devi, E. Vishnu Balan, M. K. Priyan and C. Gokulnath, “Mutual Authentication Scheme for IoT Application”, Indian Journal of Science and Technology, Vol 8. No. 26, 2015, pp. 2-5.
18. Dave Evans, “ The Internet of Things: How the Next Evolution of the Internet Is Changing Everything”, CISCO White paper, April, 2011, pp. 1-11.