Pervasive and Mobile Computing 24 (2015) 210–223

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Secure authentication scheme for IoT and cloud servers

Sheetal Kalra [a,*], Sandeep K. Sood [b]

[a] Department of Computer Science and Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab, 144001, India
[b] Department of Computer Science and Engineering, Guru Nanak Dev University, Regional Campus, Gurdaspur, Punjab, 143521, India

ARTICLE INFO

Article history:
Available online 11 August 2015

Keywords:
Authentication
Cookies
Cloud computing
Elliptic Curve Cryptography
Internet of Things

ABSTRACT

Internet of Things (IoT) is an upcoming platform where information and communication technology connect multiple embedded devices to the Internet for performing information exchange. Owing to the immense development of this technology, embedded devices are becoming more sophisticated every day and are being deployed in various arenas of life. An important advancement in today's technology is the ability to connect such devices to large resource pools such as cloud. Integration of embedded devices and cloud servers brings wide applicability of IoT in many commercial as well as Government sectors. However, the security concerns such as authentication and data privacy of these devices play a fundamental role in successful integration of these two technologies. Elliptic Curve Cryptography (ECC) based algorithms give better security solutions in comparison to other Public Key Cryptography (PKC) algorithms due to small key sizes and efficient computations. In this paper, a secure ECC based mutual authentication protocol for secure communication of embedded devices and cloud servers using Hyper Text Transfer Protocol (HTTP) cookies has been proposed. The proposed scheme achieves mutual authentication and provides essential security requirements. The security analysis of the proposed protocol proves that it is robust against multiple security attacks. The formal verification of the proposed protocol is performed using AVISPA tool, which confirms its security in the presence of a possible intruder.

1. Introduction

An embedded system is a special purpose system composed of computer hardware, software and additional mechanical components with processing capability dedicated to a specific task. Increased processing power and more sophisticated software has evolved embedded devices from single microcontroller chip with limited capabilities to multi-component intelligent systems. Single-function embedded devices have matured as "smart systems" with powerful processors, operating systems and efficient connectivity. With these smart systems, the enterprises can envision to deploy interconnected complex systems that can collect, analyze and communicate data efficiently. Presently, many organizations are trying to collaborate their embedded systems with cloud. Embedded devices can leverage vast amount of data storage and computing capability from cloud computing. Cloud computing has become increasingly popular over last few years because of its infinite resources and dynamic elasticity. The cloud technology consists of both hardware and software provided by the data center for which customers have to pay only for the resources they consume. The number of Internet connected devices is rapidly increasing and these devices not only include personal computers but also small embedded devices such as Personal

* Corresponding author.
E-mail addresses: sheetal.kalra@gmail.com (S. Kalra), san1198@gmail.com (S.K. Sood).

http://dx.doi.org/10.1016/j.pmcj.2015.08.001
1574-1192/

Digital Assistant (PDA), bank cards in the wallet and similarly many more. This evolution leads to a new scenario where Internet connected devices could benefit from cloud computing abundant resources. A networked embedded device can have capabilities based upon operations carried out in cloud and not simply restricted to its own local resources. Security still remains the major issue while getting connected to cloud for using its resources [1,2]. Embedded devices must be authenticated before getting services of a cloud and also cloud servers should be authenticated by these devices. Elliptic Curve Cryptography (ECC) is a form of public key cryptography best suited for constrained environments of embedded devices where resources like memory and processing power are very limited [3,4].

In this paper, mutual authentication scheme for embedded devices and cloud severs based on ECC has been proposed. The proposed protocol ensures mutual authentication between embedded device and cloud service provider using Hyper Text Transfer Protocol (HTTP) cookies. In Section 2, the operating environment of embedded devices connecting to cloud has been discussed. In Section 3 of the paper, the related work and security issues in collaborating embedded devices with cloud has been discussed. In Section 4, the preliminaries of ECC have been discussed. In Section 5, a novel ECC based mutual authentication protocol between the embedded device and cloud server has been proposed. In Section 6, security analysis based on an attack model has been done. In Section 7, cost and functionality analysis of the protocol has been discussed. The protocol has been formally verified using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The results have been presented in Section 8. Lastly, Section 9 concludes the paper.

2. Embedded cloud computing: operating environment

Embedded systems have become an integral and indispensable part of everyone's daily life. Embedded systems range from portable devices such as digital watches and MP3 players to complex systems like traffic lights, factory controllers, hybrid vehicles and avionics. Unlike a general-purpose personal computer, an embedded system performs one or few predefined tasks that have specific requirements and limited field configuration capability. Since the system is dedicated to specific tasks, design engineers are liable to optimize it in order to reduce the size and cost of the product. Therefore, embedded systems have limited resources available in terms of memory, CPU, screen size, limited set (or absence) of key inputs and diskless operations. These parameters play a crucial role in the design, development and testing of such systems so that it can be bound to a relatively static and simple functionality device. Cloud computing is a computing paradigm that uses Internet and central remote servers to maintain and compute multiple data applications. The latest innovations in cloud computing is to make all business applications more mobile and collaborative. Embedded devices can leverage cloud computing to expand their functionalities. Many applications in embedded systems require huge memory and processing power necessary to run complex algorithms that can generate certain results. When cloud connectivity is provided to embedded systems, the later can use resources of cloud to remotely resolve complex algorithms which reduces power consumption in embedded devices. In this way, with few resources great results can be obtained using "external intelligence" stored in cloud. The demand for Internet connected products is growing as Internet is becoming the most cost effective way of remotely monitoring and controlling embedded systems. Internet of Things (IoT) is the name used to depict a scenario where many devices are using the resources of a network without human intervention [5]. As Internet has grown rapidly, it has become the world's low cost network allowing data to be passed easily across continents. Though the embedded system applications are still growing, Internet connected embedded systems is the next step in near future. Embedded systems are generally at remote locations from people that operate them at far and distant places. In such cases, tasks like monitoring their operation, checking their performance, collecting data or upgrading application software can be a costly and time consuming process. In such a scenario, functionalities of embedded systems can be extended with cloud based data storage and computing capabilities. Also, some applications could get great benefits if they could remotely report their status, get remote data to process or even send remote messages to have their administrator informed about some incidents. However, easier said than done, security undoubtedly is the major concern while getting connected to cloud. Cloud security refers to a broad set of policies, technologies and controls deployed to protect data, applications and associated infrastructure of cloud computing. Unauthorized access raises privacy and confidentiality concerns for embedded systems using cloud computing. Security issues related to embedded devices connecting with cloud have discussed in the next section.

3. Security issues and related work

Authentication is the process of identifying legitimate entity of a particular web application. Authentication plays the most important role in successful integration of embedded devices and cloud computing services. Multitenant architecture of cloud encourages the hackers for cybercrime. Survey conducted by International Data Corporation (IDC) in 2008–2009 showed that many organizations were adopting cloud computing as it provides low cost solutions for its users [6]. Security of the information in cloud computing paradigm is still a major concern for them. There have been many cases of security attacks on well known cloud computing providers such as Amazon Web Services (Amazon S3), Google (Gmail, App Engine) and Salesforce.com [7]. In general, the major security parameters in cloud computing are authentication, confidentiality, availability, integrity and non repudiation. Researchers are continuously making efforts to develop such solutions that cater to the security needs of cloud. Recently, cloud computing services have gained a lot of popularity worldwide among business enterprises. Amazon Elastic Compute Cloud (EC2) [8] and Elastic Block Store (EBS) [9] are used to provide both storage