Physical Communication ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Physical Communication

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

Full length article

Advanced verification system using a smart card for smart city users

Trupil Limbasiya [a,*], Mihir Garg [b], Shivam Shandil [b]

Birla Institute of Technology & Science Pilani, Goa 403726, India
NIIT University, Neemrana, Rajasthan 301705, India

ARTICLE INFO

Article history:
Received 15 October 2017
Received in revised form 15 February 2018
Accepted 4 May 2018
Available online xxxx

Keywords:
Attack
Internet of Things
Smart card
Remote user
Session key

ABSTRACT

In this rapidly growing IoT (Internet of Things) environment, people avail various facilities for different intentions with the help of the Internet generally. There are many application systems, in which both (server and user) are located at separate locations. Normally, a user requests for availing diverse facilities and a server is available to provide legal services precisely. But, a server cannot grant a right of entry to any user without verifying genuinely else an adversary has many opportunities to exploit the system or users. Hence, there is a need of well-established mutual authentication framework, which can permit legal customers to access provisions and the system can be protected against multiple security attacks. In this paper, we identified that a scheme suggested by Madhusudhan et al. cannot withstand against session key disclosure, smart card lost, and includes a security flaw regarding password update. Therefore, we suggest a new authentication protocol, which can resist upon numerous security vulnerabilities and can perform the verification process within a less time period. Furthermore, the proposed protocol performs effectively in communication, storage, and energy consumption rather than other relevant authentications mechanisms.

1. Introduction

In the advanced technology-enabled world, applicants need secure and fast data access at any point for various purposes. Cloud computing is a structure to transfer information for technology related facilities based on the Internet in which assets are repossessed from the storage server over web-based tools and applications. The Internet of Things (IoT) is an inter-networking of physical/smart/connected buildings, apparatuses, and other embedded equipments, which enables these objects for retrieving and interchanging data. Cloud computing and IoT are two major architectures, which are immensely productive to various levels of Internet applicants and the combination and adoption in our daily life of these two frameworks are required to be more and more comprehensive. Before exchanging the data or getting the access from the server end, the sender and the receiver should verify each other mutually.

In order to understand the remote user authentication system, we explain two terms separately remote user and authentication. Remote user is a term used, when a user accesses or uses system resources from an off-site location where he/she is not present. Authentication refers to prove something to be legitimate or of genuine nature. It means that a person has valid credentials to have various facilities legally. It is important to note that authentication and authorization play a very different role as these two terms happen to be synonymous but are of an unequal meaning. Authorization is a process of checking the user account permissions and process of granting rights to the user for his/her account. Authentication system is a method to check the legitimacy of the particular user, who exchanges his or her credentials in the system via an insecure communication medium [1].

A remote user authentication system has two major processes. Identification states a method of making a claim towards being the legitimate user. It may seem similar to giving the correct user name but not the password also because when the password is provided it becomes part of the second process, which is verification. This method is used to check whether the credentials provided by the user are valid or not and provide accessibility of the account. But the process of authentication would not have any meaning if security is not provided against illegitimate users, who try to access resources unnecessarily [2].

Security undoubtedly is a major factor while developing an authentication system or any application. It is a key element, which should be critically analyzed and built in the system to avoid leak of vital information. It acts as an immunity system towards the attacks caused by illegitimate users. Security has many key features that sum up to its completion, first one, confidentiality in which important data should be understood only by the true user. Second being, integrity in which component of security helps

* Corresponding author at: Birla Institute of Technology & Science Pilani, Goa 403726, India.
E-mail address: limbasiyatrupil@gmail.com (T. Limbasiya).

https://doi.org/10.1016/j.phycom.2018.05.001
1874-4907/

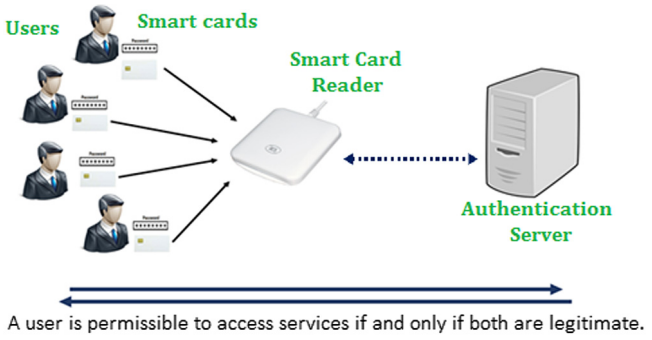

Fig. 1. Normal communication structure for authentication mechanism.

the user to determine whether the data is correct or not and third, availability, which ensures timely access to relevant resources in order to use them [3].

The remote user authentication system can have different levels of factorization to confirm the legitimation of a user and a server. Generally, it includes three types of the factor authentication system. In one factor, authentication is based only on a single factor like a text password. In two factor, authentication is based upon two factors like text password and a smart card and in three factors, authentication is based upon three factors like a text passwords, a smart card and biometric recognition. Fig. 1 dictates a general overview of the remote user authentication framework, which consists of users as service requesters, their individual smart cards, the server authority, and a smart card reader.

Our contribution: We carry out cryptanalysis of Madhusudhan et al.'s scheme [4] and found that it is not reliable for secure service management and it is weak to different attacks e.g., session key disclosure and smart card lost. In addition, we identify that the offline password change phase is computed incorrectly in [4]. Then, we propose an advance protocol to overcome these drawbacks. After that, we do security analysis of the suggested solution and emulate with other authentication mechanisms. In addition to that, we execute the suggested system to measure total compilation time and compare it with related verification models. Furthermore, we calculate battery consumption, storage cost, communication cost and compare with other related mechanisms.

The structure of this paper is as follows. Section 2 describes survey on related verification mechanisms. In Section 3, we briefly review Madhusudhan et al.'s scheme. Section 4 illustrates security flaws in the Madhusudhan et al.'s scheme. In Section 5, we propose an advanced authentication scheme. Section 6 presents security discussions on the suggested protocol. Section 7 discusses performance outcomes of the suggested system with relevant verification schemes. Conclusively, we conclude our work in Section 8.

2. Related works

Leslie Lamport [5], in 1981 introduced a remote user authentication scheme for the first time using the password table over an insecure channel. Before this, there were problems related to data, unauthorized access to system and unavailability of resources. In 1995, Wu [6] identified that scheme [5] was susceptible to some attacks (replay and impersonation) and proposed a new scheme, which was resistant against these attacks. However, Hwang et al. [7] claimed that Wu's scheme [6] was not secure against attacks (replay, impersonation and masquerade). They also proved that Lamport's scheme [5] includes security flaws like password table updation illegally. Additionally, authors [7] suggested a new scheme based on El-Gamal's public key encryption method without using the password table. In 2003, Shen et al. [8] identified masquerade attack in Hwang et al.'s scheme [7]. Furthermore, different schemes have been proposed by various scientists to protect the password focused on cryptographic techniques. But all these schemes practiced static identity, which may disclose partial statistics of legitimate individuals and has insecurity of identity theft during data transmission via a free medium. Scientists [9] explained about credentials extraction from a smart card of the users. Hence, an adversary can exploit numerous vulnerabilities.

In 2004, to avoid this problem, Das et al. [10] proposed a dynamic identity-based verification framework, and they stated that their method was protected against attacks (replay, forgery, password guessing, insider and stolen verifier). Liao et al. [11] analyzed the scheme [10] and claimed that it was susceptible to a password guessing and lack of mutual authentication. Then, they inducted their new scheme to protect observed vulnerabilities. In 2009, Wang et al. [12] identified a remote server vulnerability in [10]. Yoon et al. [13] presented that the method [11] was susceptible to attacks (reflection, insider and impersonation) and suggested an advanced method, which eliminates security flaws of [11].

In 2007, Wang et al. [14] identified that Ku et al.'s [15] and Yoon et al.'s [16] schemes are defenseless to attacks (DOS, forgery, and password guessing), and presented new scheme to remedy pitfalls of [15] and [16]. Chang and Chang [17] demonstrated that Wang et al.'s method [12] was not secured, since an attacker can favorably obtain services from the concerned authority by impersonating a permitted individual. In 2011, Awasthi et al. [18] found that Shen et al.'s [8] scheme was vulnerable to attacks (user impersonation and smart card lost) and suggested an improved method. Then, Kumari et al. [19] noticed that Awasthi et al.'s method [18] was weak to password guessing, smart card lost, absence of forward secrecy and session key. Furthermore, Kumari et al. [19] came up with its enhancement. Wen and Li et al. [20] demonstrated that Wang et al.'s method [12] was defenseless to impersonation and insider attack. Additionally, Khan et al. [21] proved that Wang et al.'s method [12] was not protected against a smart card stolen attack. After that, they presented their new and improved scheme.

He et al. [22] suggested an authentication mechanism using pairing-based cryptography to provide high efficiency. In 2014, Kumari et al. [2] demonstrated that Chang et al.'s [17] scheme was defenseless to attacks (password guessing, server masquerading, impersonation, and insider). Kaul et al. [23] pointed out that Kumari et al.'s scheme [2] was completely unsafe. An attacker can easily obtain essential parameters, common session key, password of the enrolled people and the server's secret key. They proposed their new scheme to prevail these defects. In 2016, Madhusudhan et al. [4] reviewed Wen et al.'s scheme [20] and claimed that it was vulnerable to attacks (insider, stolen smart card), and it does not achieve forward secrecy and suggested their improved method. Ali et al. [24] advised an effective verification scheme based on three-factor for multi-server systems. Amin et al. recommended a robust verification method in wireless sensor networks [25].

3. Review of Madhusudhan et al.'s scheme

Firstly, we present a scheme [4], an improved version of dynamic-identity user authentication system. It comprises of mainly four phases, being: registration, login, mutual authentication, and offline password change. The mathematical symbols have been used throughout the schemes ([4] and the proposed), which are in Table 1. Phases (registration, login, and authentication) are shown in Tables 2, 3, and 4 sequentially.

3.1. Registration phase

1. U_i initiates a registration process by selecting ID_i, PW_i, and b.