International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Smart Card

Dr. Levy M[1], *Lokanathan R*[2]

[1]Professor, Dept. of ECE, SJCIT ,Chikkaballapur, India
[2]UG Student, Dept. of ECE, SJCIT Chikkaballapur, India
drmlevyprofessor@gmail.comlokanathandhoni@gmail.com

ABSTRACT

In recent years, the internet of things has been widely utilized in various fields, such as in smart factories or connected cars. As its domain of application has expanded, it has begun to be employed using multi-server architectures for a more efficient use of resources. However, because users wishing to receive IoT(Internet of Things) services connect to multi-servers over wireless networks, this can expose systems to various attacks and result in serious security risks. To protect systems (and users) from potential security vulnerabilities, a secure authentication technology is necessary. In this paper, we propose a smart card-based authentication protocol, which performs the authentication for each entity by allowing users to go through the authentication process using a smart card transmitted from an authentication server, and to login to a server connected to the IoT. Furthermore, the security of our proposed authentication protocol is verified by simulating a formal verification scenario using AVISPA(Automated Validation of Internet Security Protocols and Applications), a security protocol-verification tool.

Keywords: User Authentication,Multi-Server, Internet Of Things, Formal Verification, Security

I. INTRODUCTION

Smart cards have been utilized excessively during the last couple of decades. In recent years though, a new generation of smart cards evolved: programmable smart cards. In this paper the authors give an overview of the current state of the technology and compare the cards on the market. The scope of uses for a smart card has expanded each year to include applications in a variety of markets and disciplines. In recent years, the information age has introduced an array of security and privacy issues that have called for advanced smart card security applications. In 1968 and 1969 German electrical engineers Helmut Gröttrup and Jürgen Dethloff jointly filed patents for the automated chip card (for details see page of Helmut Gröttrup). French inventor Roland Moreno patented the memory card concept in 1974. An important patent for smart cards with a microprocessor and memory as used today was filed by Jürgen Dethloff in 1976 and granted as USP.

4105156 in 1978. In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card. The first cards with magnetic stripes were developed by the International Air Transportation Association (IATA) in the 1970's. On this type of card the magnetic stripe stored 210 bit/inch of information, which means about 80 alphanumeric (7-bit) characters. For the sake of compatibility, today's magnetic stripes are divided into three regions. The first region corresponds to the original stripe, storing read-only information. The second region can hold additional 40 digits with an information density of 75 bit/inch. The third region is read-writeable and may contain 107 digits. According to Eurosmart, worldwide smart card shipments will grow 10% in 2010 to 5.455 billion cards. Markets that have been traditionally served by other machine readable card technologies, such as barcode and magnetic stripe, are converting to smart cards as the calculated return on investment is revisited by each card issuer year after year. A study by Dataquest in March, 2000, predicts almost 28 million smart card shipments (microprocessor and memory) in the U.S. According to this study, an annual growth rate of 60% is expected for U.S. smart card shipments between 1998 and 2003. Smart Card Forum Consumer Research, published in early 1999, provides additional insights into consumer attitudes towards application and use of smart cards. The market of smart card is growing rapidly due to its wide range of applications.

II TECHNOLOGY

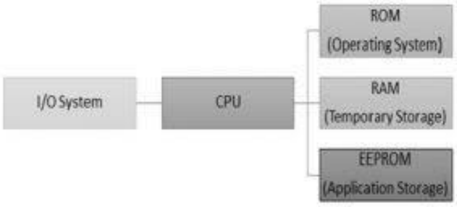

Fig 1: basic architecture of an electric module of smart card

Smart Cards are thin cards with an embedded chip, and this automatically poses its own unique challenges of architectural design. However, it turns out that the solutions tend to be a scaling down of conventional chips rather than inventing an all-new chip. This is via a single I/O port that is controlled by the processor to ensure that communications are standardized, in the form of APDUs (A Protocol Data Unit).

The operating system found on the majority of Smart Cards implements a standard set of commands (usually 20 - 30) to which the Smart Card responds. Smart Card standards such as ISO 7816 and CEN 726 describe a range of commands that Smart Cards can implement. Most Smart Card manufacturers offer cards with operating systems that implement some or all of these standard commands (and possibly extensions and additions). The relationship between the Smart Card reader and the Smart Card is a master/slave relationship. The reader sends a command to the Smart Card, the card executes the command and returns the result (if any) to the reader and waits for another command.

Microsoft released a miniaturized version of Windows for Smart Cards in late 1998, and early versions of a Gnu O/S have been released

III.Types of Smart Cards

There are two general categories of smart cards:

- contact
- contactless

Contact Smart Cards

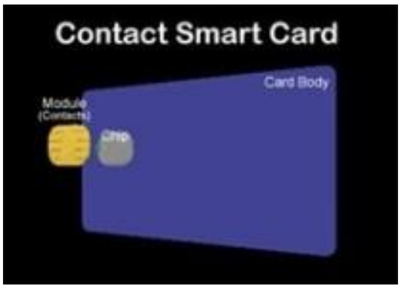

Fig 2:Contact Smart Card

Contact smart cards are **inserted into a smart card reader, making physical contact with the reader**. However, contactless smart cards have an antenna embedded inside the card that enables communication with the reader without physical contact. You tap and pay. Contactless is easy and convenient.

Contactless Card

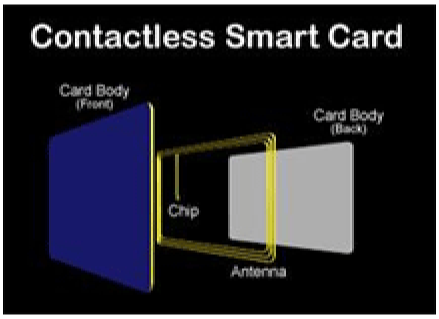

Fig 3: Contactless Smart Card

A contactless smart card is a contactless credential whose dimensions are credit-card size. Its embedded integrated circuits can store (and sometimes process) data and communicate with a terminal via NFC. Commonplace uses include transit tickets, bank cards and passports.

There are two broad categories of contactless smart cards. Memory cards contain non-volatile memory storage components, and perhaps some specific security logic. Contactless smart cards contain read-only RFID called CSN (Card Serial Number) or UID, and a re-writeable smart card microchip that can be transcribed via radio waves.

IV.CHALLENGES

Instead of carrying a bunch of different cards to an institution, a student can carry a single card that can be used to serve desired purposes like issuing books in the library, transactions in the canteen and stationery, for attendance and smart class. The project involves a card that contains a barcode which is nothing but a unique card that is assigned to the student and faculty. This project is developed to lessen the work of students. For the purpose of records, faculty have to maintain the registers for attendance, this can be replaced by the use of the smart card. One of the main challenges of the institution is to not waste electricity. Smart cards can be a major cause of saving electricity when used with IoT technology. When making payment in the institution 3rd party app or different card or cash is used which can be covered by the use of a single smart card. The upcoming future is being automated so this kind of project will make our institution look smart and reduce the time and manpower of working

V. SOLUTION

Below are some of the solutions that can be taken into consideration for the above mentioned challenges: 1. The smart card can be used to record the attendance of students. 2. The card can be used for transportation purposes, it acts like the bus pass. 3. It also serves for transaction purposes around the campus. 4. The card is also used for automation of the classroom making it a smart classroom and saving energy.

VI APPLICATION

- Mobile phones (SIM).
- public transit.
- computer security.
- schools .
- healthcare.
- Smart cards may provide strong security authentication for single sign-on (SSO) within organizations.

VII. ADVANTAGES

- High levels of security.
- Larger memory.
- Prevents fraud.
- Reliability.
- Information Security.
- Privacy.
- Ease of use.
- Reduced cost for operators and users

VIII. FUTURE SCOPE

• The future of Smart Cards is looking bright. The many existing and potential benefits smart card has to offer both the public and the private sectors of the industry raise the interests of many large corporations such as Wachovia and Motorola.

• Compared to the conventional magnetic stripe cards, smart cards offer increase security, convenience, and economic advantages.

• Reducing fraud, reducing time to complete redundant paperwork, and having the potential to have one card to access diverse networks and applications are just some of such examples

. • The discussion for the future of the smart card across the global industries can be divided into public and private sectors and are discussed below.

• Compared to the conventional magnetic stripe cards, smart cards offer increase security, convenience, and economic advantages

. • Reducing fraud, reducing time to complete redundant paperwork, and having the potential to have one card to access diverse networks and applications are just some of such examples.

XI RESULT

In recent years, as the scope of applications of IoT has broadened, the amount of data generated in IoT has become enormous, and the multi-server architecture has been utilized to manage this scenario efficiently. In a multi-server IoT environment, a user can manage and receivnformation collected by a sensor by connecting to a server via wireless networks from remote locations. However, if a malicious attacker accesses a communication network by exploiting a vulnerable authentication system, the system can be exposed to user impersonation and session key leakage attacks. Thus, a secure authentication protocol is required to prevent this. Therefore, in this paper, we propose a secure authentication protocol to analyze and respond to security threats that may occur in a multi-server IoT environment. The proposed authentication protocol has been shown to be secure against user impersonations, session key leakage attacks, as well as various other attacks. The verification properties are specified by utilizing the formal specification language HLPSL. By using the formal verification tool AVISPA, the security of the required verification properties has also been verified through the results of our experiments.

REFERENCES

1. Abdellatif R, Aslan HK, Elramly SH (2011) New real time multicast authentication protocol. International Journal of Network Security 12:13–20. https://doi.org/10.1016/j.ejrs.2011.11.003.
2. Abdellatif R, Aslan HK, Elramly SH (2011) New real time multicast authentication protocol. International Journal of Network Security 12:13–20. https://doi.org/10.1016/j.ejrs.2011.11.003.
3. http://www.ijcaonline.org/journal/number13/pxc387434. Accessed on 15/05/2022
4. http://ijtir.hctl.org/vol8/IJTIR_Article_201403012. Accessed on 15/05/2022
5. http://www.irjcjournals.org/ijieasr/Dec2013/5. Accessed on 15/05/2022
6. http://esatjournals.net/ijret/2013v02/i08/IJRET20130208042. Accessed on 15/05/2022