ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A PROPORTIONAL LEARNING ON SMART CARD AUTHENTICATION

Keziah Andrew*, M.Savitha Devi

* M.Phil Research Scolar, Asst.Professor, Department of Computer Science, Don Bosco Collage, Dharmapuri, Tamil Nadu, India

ABSTRACT

A smart card is a pocket sized card embedded with integrated circuits. Smart Cards are used in a wide range of industries worldwide to support access, identity, payment and other applications. Even though the smart cards are widely used, the hidden information can be easily read by the hackers. In order to secure the authentication, first password authentication was done. As it is very easy for the hackers to guess the password later two-factor password authentication was introduced. In that password and the users information was hidden. But this type of authentication was also not reliable. Later biometric authentication was introduced. In this type of authentication the finger print scan, retina recognition and voices were used for the means of identifying people. This type of authentication is also not reliable as there will be changes in the human body when become aged. Now another type of authentication is introduced in some of the places, that is with the help of the chip inserted in the body. It is human implantable chip known as Verichip. This article is a comparative study on the various types of smart card authentication.

KEYWORDS: *Verichip; Tracking; Hacking;Human Identification; Authentication*

INTRODUCTION

In the current world the technology has developed a lot and most of the things like e-shopping, money transfer and many other things are represented by a smart card. Smart card is activated with a password or a pin number. More the usage of smart card has developed, more illegal users also use the smart card by hacking the password or pin number. Inorder to prevent the illegal users, the smart card authentication was introduced. Smart card technology provides an excellent platform for implementing strong authentication. In addition, smart cards can support a variety of the applications used by many organizations, including password management, virtual private network authentication, e-mail and data encryption, electronic signatures, secure wireless network logon, and biometric authentication. Smart card technology is available in multiple form factors, such as a plastic card (with contact or contactless communication capabilities, or both), a USB device, or a secure element that can be embedded in a mobile phone or other device.

Fig 1 Smart Card

Types of Smart Card Authentication

Single-Factor Authentication

Single-factor authentication (SFA) is the initiative security process that requires a user name and password before granting access to the user. SFA security relies on the diligence of the user, who should take additional precautions for example, creating a strong password and ensuring that no one can access it.

Two-Factor Authentication

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it.

Biometric Authentication

Biometrics is becoming highly important in computer security world. The human physical characteristics like fingerprints, face, hand geometry, voice and iris are known as biometrics. These features are used to provide an authentication for computer based security systems [1].

Finger Print Authentication

It is known since a long time that fingerprints of humans are unique. They can be distinguished by the epidermal ridge and furrow structure of each finger, which is used to categorise fingerprints. Even identical twins don't have the same fingerprint. Fingerprints are therefore widely used to identify people since a long time. They are even accepted by law to prove evidence, which makes them a powerful tool for forensics [2].Although fingerprint biometric technology has many benefits, it also have some limiting factors. First, these devices capture not only an image of the finger, but also a picture of the dirt, greases, and contamination found on the finger. Therefore, in certain areas, there are chances of being rejected by the system if for example a worker has a mark or some other contaminants on his finger [3].

Face Recognition

The face is the commonly used biometric characteristics for person recognition. The most popular approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. As this technique involves many facial elements; these systems have difficulty in matching face images. The face recognition systems which are used currently impose a number of restrictions on how facial images are obtained. This face recognition system automatically detects the correct face image and is able to recognize the Person [4]

.

Hand Geomentry

In the hand Geomentry recognition the device is a scanner that extracts a picture of a user's hand. Some characteristics like length of the fingers, distance between them or their relative position are computed, based on the picture. These characteristics are used to match with an entry in the database. With these characteristics, you define a unique entity. That provides you unique recognition except in case of twins or even with same family members. To fool the system, you can either have a mould of the hand or just a picture of it. This method is used in some places because it is not so complex to implement [5].

Iris Recognition

In iris biometric system, an important task is to extract iris feature from a given eye image. In an eye image of a person, iris is an annular part between the pupil and the white sclera. The iris part has a number of characteristics such as freckles, corneas, stripe, furrows, crypts etc. which constitutes what is called iris features. Since iris features are distinct from one person to another these are considered in iris-based recognition process. [6].

Voice Recognition

This method is based on the recognition of someone's voice. The user speaks in a microphone, and voice is recorded and computed. It is done by using some frequency analysis of the voice. This analysis is based on how you speak and not on what you say. It can be useful to authenticate someone through a telephone, and it allows users to work on a remote location. It is less accurate than other biometrics authentication methods, and some errors can occur. This authentication method can be easily fooled by recording someone's voice. The voice recognition is used in many systems because it is cheap and easy to setup. But it can't be used as a Internet Security and Privacy [5].

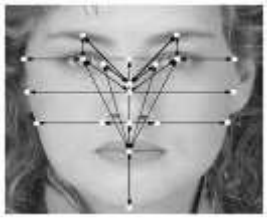

Fig 2 Face Recognition

Fig 3 Finger Print

Fig 4 Voice Recognition

Fig 5 Hand Geomentry

Veri Chip

The VeriChip is the first FDA approved human implantable radio-frequency identification microchip. The chip raises the controversy of privacy, security, health risks, and religious concerns. Speculated as a dual use "tracking device" or a denounced RFID

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

known as a "spy chip" marketed by VeriChip Corporation, the invisible to the naked eye 16 digit frequency responder can be held as identity verification, medical record access and more [7]. The tube-shaped VeriChip includes a memory that holds 128 characters of information, an electromagnetic coil for transmitting data and a tuning capacitor, all encapsulated within a silicone-and-glass enclosure. The passive RF unit, which operates at 125 kHz, is activated by moving a company-designed scanner within about a foot of the chip, enabling it to transmit data [8].


Fig 6 Verichip *Fig 7 Verichip inserted Hand*

RFID

Radio frequency identification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. RFID tags contain antennae to enable them to receive and respond to radio-frequency queries from an RFID transceiver.

The RFID system comprises the tag, reader, backend database, and or control unit. The tag comprises a radio frequency chip, encoding and decoding circuitry, antenna unit, and or a memory unit. Depending on power capacity, a tag can be classified into passive, semi-active or active tag.Tags without internal power supply, are called passive tags, tags without internal power supply but only uses the internal supply for its internal memory circuitry are called semi-active, while tags that uses its internal power unit to power both its internal circuitry and the antenna unit for communication are called active tags. Additionally, tags can be categorized based on their frequency of communication. The communication frequency between the tag and the reader determines the energy and read range, and in some instance, the size of the tag. The reader communicates with the tag through tag interrogation [9].

Applications of Verichip

The Verichip is widely used in the medical field. The chip used for medical purposes is known as Verimed. The verichip is also used to track the criminals. RFID technology for human implants is generally based on battery-less (passive) devices and allows achieving very short read range, typically 10cm or much less. Consequently RFID implants cannot communicate with GPS satellites that would be required for the real-time tracking of a person. RFID technology is then not suitable for the real–time tracking of a person anywhere on the planet through RFID-chip deeply implanted in his body. The remote control of human biological functions by using RFID technology seems to be more realistic. Following the estimations of Burke et al. [Burke 2009], a single chip including antenna radio system with on-board sensors of size 100 × 100 × 1 μm3 seems to be feasible with available technology. Consequently, the wireless communication with small RFID implants in humans for reading information about chemical or physical quantity in biological systems or for providing the remote activation/deactivation of biochemical aWith RFID technology, library Inventory can be fast and efficient [10].

The recent biometric technology is brain wave pattern recognition. In which the Sensors able to identify individuals' brain patterns and heart rhythms could become part of security systems which also use more traditional forms of biometric recognition. The advantage of brainwave signals is that they vary from person to person, even when they think alike. Everyone's brainwave signal is a bit different even when they think about the same thing. They are unique and cannot be faked. Hence now it can used for person authentication and sperson identification. Person authentication aims to accept or to reject a person claiming an identity, i.e., comparing a biometric data to one template, while the goal of person identification is to match the biometric data against all the records in a database.Hence a more efficient method than brain wave recognition is thus provided by this Verichip or VeriMed [11].

Fig 8 Brain wave Recognition

Verimed

There is a wide array of medical uses for microchip implants. One example is using the implants with prosthetics. An RFID chip could be placed on top of the brain to improve movement or functionality of the prosthetic. With the implant, the person would have both input and output capabilities. The

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

downside to the brain implant is that the operation is more invasive. As an alternative, doctors could place an electrode on the limb itself that would act on electrical impulses from the brain. The operation is less invasive, but the electrode would have very limited input capabilities [12].

Veripay

Bio-chip implant "VeriPay" is for cashless and Checkless society. At a global security conference held on November 21, 2003, in Paris, an American company, Applied Digital Solutions, announced a new syringe-injectable microchip "VeriPay" implant for humans, designed to be used as a fraud-proof payment method for cash and credit-card transactions.

The chip implant is being presented as an advance over credit cards and smart cards, which, absent biometrics and appropriate safeguard technologies, are subject to theft, resulting in identity fraud. Cash less payment systems are now part of a larger technology development subset. Government identification experiments that seek to combine cashless payment applications with national ID information on media (such as a "smart" card), which contain a whole host of government, personal, employment and commercial data and applications on a single Contactless chip.

Fig 9 VeriPay

RFID for tracking the criminals

The Verichip is also widely used to track the criminals. An RFID anklet is weared on the criminals. With the help of this the criminals could be tracked where ever they go. This prevents the criminals to escape from the prison.

Fig 10 RFID for criminals

CONCLUSION

In this article we have analysed the Proportional Learning of Smart card Authentications and a new type of authentication that is the Human implantable chip. And also we have analysed the applications of the RFID Chip.

FUTURE ENHANCEMENT

In the present world most of the people have switched on to the credit card and debit card transactions for their purchasing. But in most of the cases it could be stolen or damaged. Inorder to get rid of such problems the implantable chip could be used for money transfer during buying and selling. In the future, it is possible to live in a money free world that is instead of Credit Card Verichip could be used as everything could be embedded in the chip.

REFERENCES

1. Sulochana sonkamble, Dr. Ravindra thool, Balwant sonkamble, 1Asstt Prof., Department of Information Technology , MMCOE, Pune, India-411052 2Professor, Department of Information Technology, SGGSIE&T,Nanded, India -411017 3Asstt Prof., Department of Computer Engineering, PICT, Pune, India-411043. Survey of Biometric Recognition Systems and their applications. 2010.
2. Birgit Kaschte Computer Science department University of Auckland birgit@kaschte.de. Biometric authentication systems today and in the future. 24 October 2005
3. Fingerprint Biometric Technolog, Disadvantages of Fingerprint Biometric Devices. Wednesday, April 7, 2010.
4. Sulochana Sonkamble, Dr.Ravindra Thool, Balwant Sonkamble Asstt Prof., Department of Information Technology , MMCOE, Pune, India-411052 Survey of Biometric Recognition Systems and their Applications. 2005 – 2010 JATIT.
5. Professor: Johan Montelius Autumn Semester 2005 Assignment 1, Biometric authentication, Internet Security and Privacy. 2G1704 Alexandre Fustier Vincent Burger Internet Security and Privacy. 2G1704 Professor : Johan Montelius Autumn. Internet Security and Privacy , 2G1704, September 2005
6. V´aclav Maty´aˇs and Zdenˇek ˇR´ıha Faculty of Informatics, Masaryk University Brno, Czech Republic {matyas, zriha}

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

@fi.muni.cz . Biometric authentication security and usability.
7. Eric Kincaid, 20092 VeriChip RFID Microchip. TED- 111, March 31.
8. Charles J. Murray. Injectable chip opens door to 'Human Bar Code' .
9. Ikuesan R. Adeyemi Norafida Bt. Ithnin , raikuesan2@live.utm.my afida@utm.my Department of Computer System and Communications, Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia.. Users Authentication and Privacy control of RFID Card.
10. Hervé Aubert, Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) – CNRS And University of Toulouse: INP, UPS, INSA, ISAE, 7 Avenue du colonel Roche, Toulouse, France. RFID Technology for Human Implant Devices Technologie RFID pour implants dans le corps Humain.
11. K. Nithiya Department of Applied Electronics , IFET college of Engineering, Villupuram, India .Emerging Trend of Being Chipped in the Headbrain Implant Using Biometric Verimed - Positive ID. Volume 4, Issue 4, April 2014.
12. Charles Smith (1). Human Microchip Implantation.