Access Control Verification System using Statistical Methods

Khaing Thanda Swe

Mandalay Technological University, Mandalay,Myanmar

Abstract

Currently, most of the people in the developing countries are using paper-based personal identification cards. These cards may make unauthorized card creation and unauthorized card holder reading. This paper aims to overcome these limitations; unauthorized card creation and fault card holder reading. The other objectives of this system are to give more accurate, faster transaction times and reliability. This system is divided into two modules. The first module is that RFID technology is used for ensuring either the id-card is valid or not. And then, ECC digital signature is applied for ensuring whether id-card is driven from authorized person or from authorized party. The second module is that iris recognition is used to make sure the card holder is either authenticated person or not. The whole system mainly aims to give the card validation and person authentication. B

Keyword: RFID, id-card, ECC

1.INTRODUCTION

While the technology has been available for several decades, the 21st century has marked the beginning of a new era in RFID development and usage. The major driver for its development has been the tagging of physical objects- people, places, and things- with single chip radios so they can interface with computers. RFID systems are short-range, low frequency, low bit-rate wireless networks. Since their origins are in the late 1940s, they have been developed specifically to exchange small amounts of data over relatively short distances using tags and readers based on proprietary air interface protocols, and more recently ISO and EPC standards. RFID is increasingly being used to enhance the authenticity of individual forms of identification without creating longer ID authenticity verification wait times.

This system is intended to develop with two phases: card validation and person authentication. On card validation, there is able to validate either the card is valid or is driven from authenticated party by applying RFID techniques and ECC digital signatures. On the person authentication, there is whether the card holder is authentic person or not. This system implements one new way using correlation method for iris recognition when checking the person is authentic or not. Moreover, this system gives fairness property because there is no human error or interruption.

2. LITERATURE SURVEYS

Contactless payment applications have existed for more than a decade. Since the 1980s, millions of toll-road users have used "long distance" contactless technology for prepaid accounts or customer billing. ExxonMobil's Speed pass was introduced in the mid-1990s, and over 6 million customers now use a key fob, vehicle tag or watch to pay for gas and convenience store items at more than 7,500 Exxon and Mobil stations in the United States, Canada, and Singapore. Currently, most of the people around the world are using the contactless id-card system to fulfill the requirements and get the required information sources

Radio Frequency Identification (RFID) system is rooted in discoveries made by Faraday during the mid-nineteenth century and discoveries made between 1900 and 1940 in radio and radar technologies. The latest indication that RFID is becoming the enabling technology of the 21st century is the course that the world's biggest retailer and logistics juggernauts have chosen. Both Wal-Mart and the U.S. Department of Defense (DOD) intend on fully incorporating RFID into their supply chain and logistics. More to the point, Wal-Mart will require its top 100 suppliers to use RFID

tagging of each item addition to each pallet. Trials started in Dallas in January 2005 [1].

In 2012, Nurbek Saparkhojayey and Selim Guvercin in [2] proposed a system that checking students' attendance is one of the most important issues for universities, because many universities evaluate students' attendance and while giving the final grade, professors consider their total number of appearances on classes during the whole semester. This brings to the idea of having some tool to control students' attendance. After thinking all these issues, authors of the following research paper decided to create a system that makes easier to check students' attendance automatically. The system is based on RFID technology. Each card has a unique ID, precluding the duplication of a card. This means no class time will be wasted.

The digital personal identification system was the result of some visionary thinking by people in the early 21st century that saw great potential value in allowing computers to share information on research and development in scientific and military fields. In 1998, W.W.Boles and B.Boashash in [3] reported a new algorithm for recognizing the iris of the human eye based on the wavelet transform is presented. It uses only a few selected intermediated resolution levels for matching, thus making it computationally efficient and less sensitive to noise and quantization errors. The proposed iris recognition system is designed to handle noisy conditions as well as possible in illumination and camera-to-face distances.

Although significant progress has been achieved iris recognition, some problems remain unsolved. To evaluate the performance of the existing iris recognition algorithms and provide more knowledge of essential information of iris characteristics, larger iris databases are needed. In 2011, P.P.Chitte, J.G.Rana, R.R.Bhambare, V.A.More, R.A.Kadu and M.R.Bendre in [10] focused on the construction of iris databases with synthesis method. The objective of this system was to produce a working prototype program that functions as an iris recognition tool using the algorithms described by Professor John Daugman and other techniques in order to implement this in an accurate and useful way that is also user-friendly. In this paper, an iris image synthesis method based on Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Daugman's rubber sheet model is proposed [4].

In 2012, Pankaj P.Chitte, J.G.Rana and Sachin Taware in [5] proposed an iris image synthesis method based on Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Daugman's rubber sheet model & hybrid model. Here, different techniques i.e. ICA,PCA, Daugman's rubber sheet model & hybrid model which is combination of all above three along with RFID system are compared. After using lot many algorithms for iris recognition, Daugman's rubber sheet model is better. And if distance between input error and validation error for image is small then performance is good and performance is poor for large distance.

The author in [6] proposed a system that bus detection device for the blind using RFID application. This system outlines a bus mechanism for the blind people in going on a voyage. In order to get transportation independently, the blind people use auditory touched clues like walking stick or white cane. The limitation of the walking stick is that a blind person must come into enclosed area of their surroundings to determine the location of any trouble. For that basis, various devices have been developed the Sonicguide, the Mowat sensor, the laser cane and the Navbelt. Nevertheless, these devices can only assist the blind at a pedestrian crossing.

The author in [7] implemented a system that a smart hospital using RFID technologies. RFID is a rapid development and also healthcare is predicted to be one of its main growth areas. This paper discusses how the revealing technology can be utilized to build a smart hospital and how to use an assets tracking application called the RFID Locator, to increase the quality of the hospital services. Really, by the combination in mobile devices in eHealth applications, RFID supports optimizing business process in healthcare and improve patient safety.

The author in [8] discusses a method and system for identifying and tracking persons using RFID-tagged items carried on the persons. Previous purchasing records for every person who shops at a retail store are collected by POS terminals and stored in a transaction database. When a person holding items having RFID tags enters the store or other designated area, a RFID tag scanner located therein scans the RFID tags on that person and reads the RFID tag information. The RFID tag information collected from the person is correlated with transaction records stored in the transaction database according to known correlation algorithms. The exact

identity of the person or certain behavior about the person can be determined. This information is used to monitor the movement of the person through the store or other areas.

3. BACKGROUND THEORY

This section introduces some basic principles of RFID techniques, digital signature among cryptographic techniques, advantages of ECC digital signature over others, and presents the working principles of ECC digital signature and MD-5 hash function to get authentication service for a secure digital personal identification system. Finally this section discusses the iris recognition system for person authentication.

3.1. Radio Frequency Identification

RFID technology enables the optimization of multiple business process through the improvement, the automation or even the elimination of existing processes, and the emergence of new processes called intelligent processes or smart processes, which are automatically triggering actions or events.

The major areas that have driven the commercial deployment of RFID technology are logistics, supply chain management, library item tracking, medical implants, road tolling (e.g., E-Z Pass), building access control, aviation security, and homeland security applications. These systems are used for a wide range of applications that track, monitor, report, and manage items as they move between different physical locations. From inventory management to theft detection, RFID has been applied in many areas such as in the automotive industry and logistics, as well as in warehouses and retail stores. Most cars are equipped with a remote control to open and lock a door. Money cards are used for public transportation payments. Although there is no RFID association in their names, both a car remote control and money cards are RFID applications. RFID technology has become more and more widely used in real-world applications without people realizing it.

Although current state-of-the-art receiving systems are highly optimized by using bar coding and wireless communications to a central computer, the process is error-prone and time-consuming because of human intervention. RFID presents security and privacy risks that must be carefully mitigated through management, operational, and technical controls in order to realize the numerous benefits the technology has to offer [9].

3.1.1. Working Flow of RFID

RFID is a genetic term for technologies that use radio waves to automatically identify people or objects. Unlike bar codes, no clear line of sight is required to obtain an accurate read. The basic RFID system comprises a transponder, a reader and an antenna. Data is stored in a transponder device called a tag. Current tags, depending on application, can hold up to 2k bits of data. Tags can be read-only or read/ write.

A radio frequency signal is transmitted from the reader to a transponder that passes within range of the reader's antenna. The signal triggers RF emissions from the tag. The transponder holds bits of data, which is either reflected or sent back to the reader, depending on whether the tag is passive or active. Transponder data includes information such as the transaction record type, the unique transponder ID number, the reader ID number, the transaction status code, and the error detection code. Customer data can be specified as well.

One of the main hurdles for the widespread adoption of RFID systems is privacy concerns. The concerns become particularly salient as the retail industry contemplates moving from pallet and crate tagging to individual item tagging. RFID use substantially differs from that of other systems. The tag has a close association with the item it identifies. Moreover, the sensitive information usually does not pertain to the tag itself but to the item. This close association between the tag and the item that it identifies gives rise to novel threats such as tracking that are not usually addressed in conventional security systems.

To be economically viable for most applications, the tag is not allowed to posses sophisticated data processing capabilities. Thus, the design of security protection for RFID systems is challenging. For example, extensive cryptosystems such as AES, DES, ECC, or high-quality random number generators may not be available on the tag. Hence, a substantial amount of recent research effort has been dedicated to design security techniques with sufficiently low overhead to be feasible on RFID systems [10].

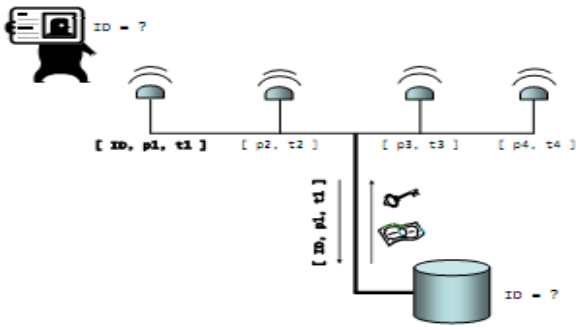

Figure1. Working Flow within RFID System [10]

3.2. Digital Signature Algorithm

There are three types of encryption techniques in RFID. These are:

- Public Key Encryption
- Common Key Encryption
- Hash Function

3.2.1. Public Key Encryption

Kinoshita et al. propose the internal re-encryption scheme, which uses a public key encryption. In this scheme, a public key encryption function and an NVRAM are embedded within each RFID tag. The encrypted ID stored in the NVRAM is re-encrypted by the public key encryption function on the RFID tag. Since the tag changes its output every time, this scheme provides good personal information protection. However, there is the problem that the tag is expensive because a public key encryption function is complex and costly [11].

3.2.2. Common Key Encryption

Kinoshita et al. propose the common key encryption scheme, which uses a common key encryption. In this scheme, a common key encryption function, a ROM and a pseudorandom number generator are embedded within each RFID tag. The server identifies the tag through the following protocol.

Step 1: RFID tag T_i generates a random number R, and sends $X= E_k (id_i || R)$ to the server.

Step 2: The server decrypts X using the common key K and gets id_i.

The calculation of the common key encryption is smaller than that of the public key encryption; however, it is vulnerable to tampering because the common key must be shared among all tags. The reason why the common key must be shared is as follows. If each tag uses an individual key, the server must know which key to use for decrypting of the encrypted ID. Therefore, it is difficult to use individual common keys [11].

3.2.3. Hash Function

Hash-based schemes use a hash function as a cryptographic function. Since the hash calculation is a lightweight operation, the hash-based schemes are suitable for RFID systems, where the implementation cost of an RFID tag must be low. However, the calculation load of the server is high because the server needs to do an exhaustive search [11].

3.2.4. MD5 Message Digest

MD5 was designed to be somewhat more "conservative" than MD4 in terms of being less concerned with speed and more concerned with security. It is very similar to MD4. The major differences are:

- MD4 makes three passes over each 16-byte chunk of the message. MD5 makes four passes over each 16-byte chunk.
- The functions are slightly different, as are the number of bits in the shifts.
- MD4 has one constant which is used for each message word in pass 2, and a different constant used for the entire 16 message words in pass 3. No constant is used in pass 1.

MD5 uses a different constant for each message word on each pass. Since there are 4 passes, each of which deals with 16 message words, there are 64 32-bit constants used in MD5. The 64 values (in hex) are:

T_1 = d76aa478	T_{17} = f61e2562	T_{33} = fffa3942	T_{49} = f4292244
T_2 = e8c7b756	T_{18} = c040b340	T_{34} = 8771f681	T_{50} = 432aff97
T_3 = 242070db	T_{19} = 265e5a51	T_{35} = 6d9d6122	T_{51} = ab9423a7
T_4 = c1bdceee	T_{20} = e9b6c7aa	T_{36} = fde5380c	T_{52} = fc93a039
T_5 = f57c0faf	T_{21} = d62f105d	T_{37} = a4beea44	T_{53} = 655b59c3
T_6 = 4787c62a	T_{22} = 02441453	T_{38} = 4bdecfa9	T_{54} = 8f0ccc92
T_7 = a8304613	T_{23} = d8a1e681	T_{39} = f6bb4b60	T_{55} = ffeff47d
T_8 = fd469501	T_{24} = e7d3fbc8	T_{40} = bebfbc70	T_{56} = 85845dd1
T_9 = 698098d8	T_{25} = 21e1cde6	T_{41} = 289b7ec6	T_{57} = 6fa87e4f
T_{10} = 8b44f7af	T_{26} = c33707d6	T_{42} = eaa127fa	T_{58} = fe2ce6e0
T_{11} = ffff5bb1	T_{27} = f4d50d87	T_{43} = d4ef3085	T_{59} = a3014314
T_{12} = 895cd7be	T_{28} = 455a14ed	T_{44} = 04881d05	T_{60} = 4e0811a1
T_{13} = 6b901122	T_{29} = a9e3e905	T_{45} = d9d4d039	T_{61} = f7537e82
T_{14} = fd987193	T_{30} = fcefa3f8	T_{46} = e6db99e5	T_{62} = bd3af235
T_{15} = a679438e	T_{31} = 676f02d9	T_{47} = 1fa27cf8	T_{63} = 2ad7d2bb
T_{16} = 49b40821	T_{32} = 8d2a4c8a	T_{48} = c4ac5665	T_{64} = eb86d391

3.2.5. ECC Digital Signature

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller and Neil Koblitz as an alternative mechanism for implementing public key cryptography. Unlike RSA, ECC is based on the problem of finding discrete logarithms over a finite field. Due to its small key size and conventional mechanism, ECC has been commercially accepted. ECC is based on elliptic curves that are typically defined over either the integers modulo a prime number (GF(p)) or over binary polynomials. When referring to the key size, it means the size of the prime number or binary polynomials in bits. Because of the much smaller key sizes involved, ECC algorithms can be implemented on smart cards without mathematical coprocessors. Contactless smart cards work only with ECC because other systems require too much induction energy. Since shorter key lengths translate into faster handshaking protocols, ECC is also becoming increasingly important for wireless communications.

The elliptic curve analogues of the older discrete algorithm (DL) cryptosystems are replaced by the group of points on an elliptic curve over a finite field. The mathematical basis for the security of elliptic curve cryptosystems is the computational intractability of the elliptic curve discrete logarithm problem (ECDLP). ECC is a relative of discrete logarithm cryptography. An elliptic curve E over Z_p as in Figure 3.8 is defined in the Cartesian coordinate system by an equation of the form.

ECC digital signature schemes can be used to provide the following basic cryptographic services:

- data integrity (the assurance that data has not been altered by unauthorized or unknown means)
- data origin authentication (the assurance that the source of data is as claimed)
- non-repudiation (the assurance that an entity cannot deny previous actions or commitments)

$y^2 = x^3 + ax + b$

Each value of a and b gives a different elliptic curve. The public key is a point on the curve and the private key is a random number. The public key is obtained by multiplying the private key with a generator point G in the curve.

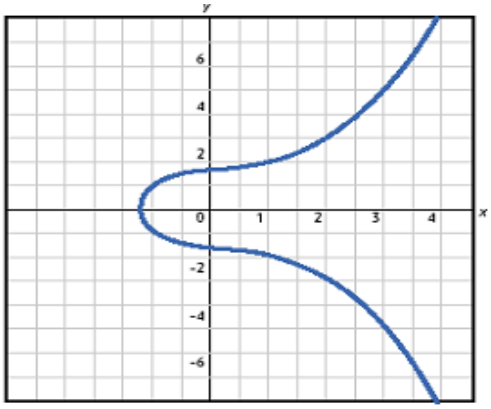

Figure 3.8. An Elliptic Curve [12].

3.2.6. Iris Recognition

Like a retina scan, an iris scan also provides unique biometric data that is very difficult to duplicate and remains the same for a lifetime. The scan is similarly difficult to make (may be difficult for children or the infirm). However, there are ways of encoding the iris scan biometric data in a way that it can be carried around securely in a "barcode" format.

This recognition method uses the iris of the eye which is colored area that surrounds the pupil. Iris patterns are unique and are obtained through video based image acquisition system. Each iris structure is featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings. An IRIS Image is shown in Figure 2.

Figure 2. Image of IRIS [13]

4. Proposed Verification System with Statistical Methods

The proposed system is divided into two modules. The first module is the card validation. For card validation, ECC digital signature must be put into the RFID card. A key evolving signature scheme contains a key generation algorithm, a signing algorithm, and a verification algorithm. The public key is also changed with the private key throughout the lifetime of the scheme, making the verification algorithm very similar to that of a standard signature scheme. A key-evolving signature scheme has its operation divided into time periods, each of which uses a different secret key to sign a message. Then this signature is set into the RFID card. When the person comes in, the RFID reader reads the digital signature from the card. If the signature matches, the card is valid.

The second module is the person authentication. For person authentication, the card holder's iris code must be drawn by using correlation method. This iris code must be put into the RFID card. When the person comes in, the RFID reader reads the iris code from the card. If the iris code from the card matches with the iris code form the database, the person is authentic. If the card holder satisfies the above two modules, the card holder is allowed to be permitted.

Feature extraction is a special from of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant (much data, but not much information) then the input data will be transformed into a reduced representation set of features (feature vector). Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen, it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input.

After edge detection, inner and outer edges of iris as well as pupils area are achieved. Using the center of pupil and inner edge, various sizes of lines like along concentric circles can be drawn which statistical features are computed.

Skewness: The skewness is the measurement of the inequality of the intensity level distribution about the mean. The value can be positive or negative.

Positive: Large number of intensity values is on the right side of the mean.

Negative: Large number of intensity value is on the left side of the mean.

Zero: Distribution of intensity values is relatively equal on both sides of the mean.

$SKEW = [\sum(b\text{-}mean)^2\ p(b)]/\ (stddev)^3$

Kurtosis: The Kurtosis measures the peak of the distribution of the intensity values around the mean. The high value of Kurtosis indicates peak of the distribution is sharp. The low value of Kurtosis indicates the peak of the distribution is rounded.

$Kurtosis = [\sum(b\text{-}mean)^2\ p(b)]/\ (stddev)^4$

Energy: Energy measures the uniformity of the intensity level distribution. If the value is high, the distribution is to a small number of intensity values.

$ENERGY = \sum [p(b)]^2]$

Entropy: The entropy measures the randomness of the distribution of the coefficients values over the intensity levels. If the entropy is high, then the distribution is among more intensity levels in the image. This measurement is the inverse of energy.

$ENTROPY = \sum p(b)]\ \log_2 [p(b)]$

Smoothness: Smoothness measures the intensity value by using the standard deviation value.

$SM = 1\text{-}\ (1/(1+(stddev)^2))]$ [13Som] [14]

Methods	Feature Extraction (ms)
Daugman	682.5
Boles	170.3
Li Ma	244.2
Y. Wang	426.8
Proposed	182.0

Table1. Comparison of proposed system with feature extraction time

5. Experimental Results

The proposed system has to do two works. From the two works, one work is to get iris code and the second work is to achieve digested message and digital signature. Then, these data are stored in the database and also written onto the RFID card.

The advantages of the system are that the system can easily check the incoming person is authentic person or not. Only the authenticated person can perform the required tasks that they want to do. Anyone cannot pretend on behalf of others. The system checks that both personal identification card and person are sure or not. So, the system can save time and get user satisfaction while using this system. This system is replaced the paper-based personal identification system with digitized personal identification system.

This system supports the Contactless Personal Identification system to be more convenience to the users. Computerized calculation is very beneficial in many areas. It can also be used in the following applications:

- Learning and applying the ECC digital signature into the RFID technique
- Getting the unauthorized card creation and unauthorized card holder reading
- Giving the guarantee whether the person is either authentic or not
- Performing the security for data access control
- Retrieval of the information about the users
- Updating the users information if necessary

So, it also gives user satisfactions with full performance in during using the system.

6.ACKNOWLEDGEMENT

The author wishes to her special thanks to her principal, Dr. Sint Soe, Rector of Mandalay Technological University, for his invaluable suggestion, leading and helpful guidance during the period of study. The author would like to heartfelt thanks to all her teachers throughout her life to prepare this research paper without any trouble.

REFERENCES

Article/ Research Paper

[1] *The State of RFID Implementation and Its Policy Implications*: An IEEE-USA White Paper, 15 April 2009.

[2] W.W.Boles and B.Boashash.: "*A Human Identification Technique using Images of the Iris and Wavelet Transform*". IEEE Transactions on Signal Processing, 46(4), April 1998.

[3] Mr.P.P.Chitte, Prof.J.G.Rana, Prof.R.R.Bhambare, Prof.V.A.More, Mr.R.A.Kadu, M.R.Bendre.: "*Iris Recognition System using ICA, PCA, Daugman's Rubber Sheet Model Together*". International Journal of Computer Technology and Electronics Engineering, 2(1), 2011.

[4] Pankaj P.Chitte, J.G.Rana, Sachin Taware.: "*Advanced Security System using ICA, PCA, Daugman's Rubber Sheet Model Together*". International Journal of Computer Applications, 48(13), June 2012.

[5] Debnath et al.: *Biometric Authentication: A Review,* International Journal of u- and e- Service, Science and Technology, 2(3), September, 2009.

[6] S.S. Kullarni et al.: *An Efficient Iris Recognition Using Correlation Method,* International Journal of Information Retrieval, ISSN: 0974-6285, 2(1), Page 31-40, 2009.

[7] Vaclav Matyas and Zdenek Riha.: *Biometric Authentication- Security and Usability,* Faculty of Informatics, Czech Republic, 2004.

Books

[1] C. Diaz (Ed.) et al.: *Advanced Applications for e-ID Cards in Flanders,* ADAPID Deliverable D2, Requirement Study, April 2006.

[2] Emmett Erwin, Christian Kern.: *Radio Frequency Identification in Libraries*, March 2005, 18 (1).

[3] *Contactless Payment and the Retail Point of Sale*: Applications, Technologies and Transaction Models, A Smart Card Alliance Report, March 2003, PT- 03002.

[4] Gildas Avoine.: *Rfid security and privacy lounge*, http://www.avoine.net/rfid/, 2009.

[5] James Wayman, Anil Jain, Davide Maltoni and Dario Maio.: *An Introduction to Biometric Authentication Systems,* 2004.