Advancement Of Digitized Identification System With Biometric Techniques

Khaing Thanda Swe, Myo Hein Zaw

Abstract: - Currently, RFID is a well-known topic for enhancing the authenticity of individual forms of verification. Most of the human beings in the developing countries are using on paper personal identification cards. These cards may make unlicensed card creation and forbidden card holder reading. The proposed system aims to overcome these limitations; card creation and card holder reading. The other objectives of this system are to give more precise, rapid transaction times and credibility. This system is divided into two parts. The first part is that RFID technology is used for ensuring either the id-card is genuine or not. The second part is that iris recognition is used to make sure the authenticated person. The whole system mainly aims to give the card validation and person authentication. Based on the experimental and theoretical results, better suited new solutions that overcome relevant privacy needs will be proposed.

Index Terms: - ECC, id-card, iris recognition, RFID

————————————◆————————————

1 INTRODUCTION

Nowadays, radio frequency identification system is growing excessively by improving in manufacturing techniques and successful data-handling methodologies. While the technology has been achievable for various decades, the beginning of a new era in RFID development and usage has been recorded in the 21st century. The major advantage of enabling RFID for trailing objects is its ability to sustain adequate identification. Since the RFID system's origins are in the late 1940s, the small amount of data over relatively short distances and more recently ISO and EPC standards. RFID is increasingly being utilized to improve the authenticity of individual forms of identification without creating longer ID authenticity verification wait times. The proposed system is intended to develop with two parts: 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 both 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 for iris recognition using correlation method when checking the person is authentic or not. Moreover, this system gives fairness property because there is no human error or interruption.

2 RELATED WORKS

Today, advanced digitized systems are being used by many people who want to access immediately the acquired information about their applications and needs due to the rapid accessible of the technology. The rapid growth of digitized system provides highly customized, accessible and interactive sources of information and has created huge demand for applications.

————————————————————————

- Khaing Thanda Swe is currently pursuing PhD degree program with Information Technology Engineering at University of Technology (Yatanarpon Cyber City), Myanmar, PH-0952018970.
  E-mail: khaingthandasweutycc@gmail.com
- Myo Hein Zaw is currently pursuing in Information Technology Engineering as a Principal in Computer University (Monywa), Myanmar, PH-0952132113.
  E-mail: mheinzaw@gmail.com

The author in [1] 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 [2] 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 [3] 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. But most of the existing methods have limited abilities in recognizing relatively complex features in realistic practical situations. However, these methods are usually not reliable. To increase the level of security, the proposed system is carried with the combination of IRIS recognition unit and RFID unit. As a new branch of biometrics, iris recognition shows satisfactory performance. Compared with other biometric features, personal authentication based on iris recognition can obtain high accuracy due to the rich texture of iris pattern.

3 THEORETICAL BACKGROUND

This section discusses some basic principles and advantages of RFID techniques, ECC digital signature among cryptographic techniques and presents the idea of connecting RFID and ECC digital signature together to get authentication service for a secure digital personal identification system.

3.1 RFID System Components

Modern RFID system has three major components:

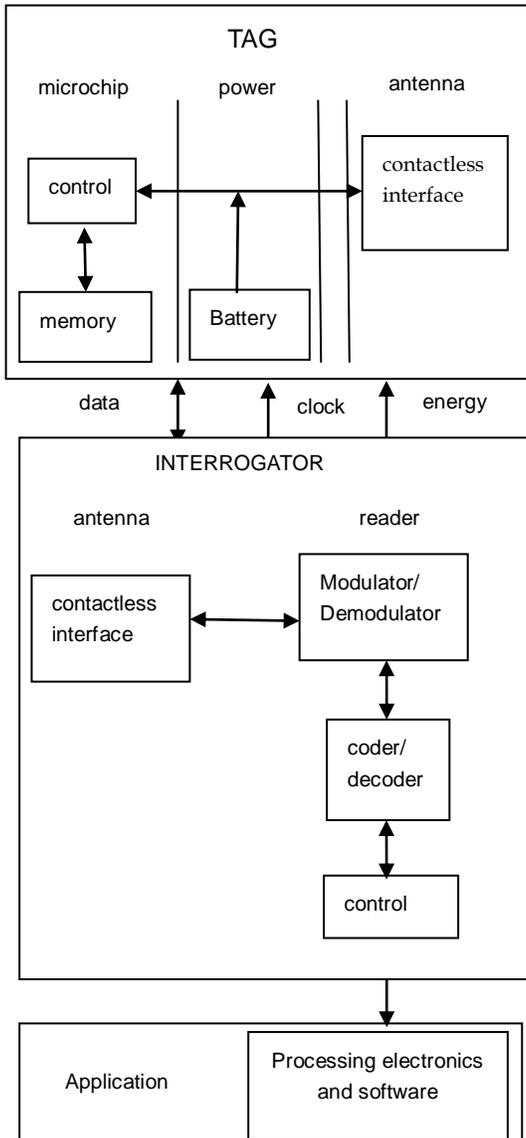- Tag- Transponder
- Reader- Transceiver
- Backend Database

Figure1. RFID System Component

3.2 Security Issues

There are many security issues related to RFID. They can be broadly divided into following categories.

- **Tag Access**
  - ➢ Physical Access
  - ➢ Counterfeiting
  - ➢ Eaves dropping
  - ➢ Traffic Analysis

- ➢ Denial of Service Attacks

- **Tag Collision**
  - ➢ Binary tree-walking scheme [4]

3.3 Advantages of RFID

While the bar code is widely accepted in the marketplace, RFID offers some distinct benefits:

- ➢ No "line-of-sight" requirements
- ➢ More automated reading
- ➢ Less labor required
- ➢ Improved read rates
- ➢ Larger data capacity
- ➢ Ability to "write" information on a tag
- ➢ Effectiveness in harsh environments (e.g., temperature extremes, dusty and dirty conditions) [5].

3.4 ECC Digital Signature

Elliptic curve cryptosystem (ECC) were invented by Neal Koblitz and Victor Miller in 1985. They can be viewed as elliptic curve analogues of the older discrete logarithm (DL) cryptosystems in which the subgroup of Z_p is 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 ellipitic curve E over Z_p is defined in the Cartesian coordinate system by an equation of the form:

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

Symmetric Encryption Key Size	RSA and Diffie-Hellman Key Size	ECC Key Size
80	1024	16
112	2048	22
128	3072	25
192	7680	38
256	15360	51

Table1. Comparison of key sizes [6].

4 IRIS RECOGNITION

Currently, biometric recognition is a usual and trustworthy way to prove that a document is authentic and a forgery the individuality of a living person based on physiological or behavioral characteristics. A physiological trait is proportionately resistant to change bodily or natural attributes, such as fingerprint, iris pattern, facial feature, hand silhouette, etc. This measurement is essentially the same and cannot be changed without enormous pressure. Human iris pattern of personal biometric authentication technologies is excellently

fitted to be implemented to any high level of security access control system. The possibility of two people with the pattern of the iris is closely nullified. This is why the iris identification technique has turned into a vital biometric answer for people to recognize the network access control to computer applications In iris recognition, although significant improvement has been made, a number of issues remain unanswered. To appraise the performance of the existent iris recognition algorithms and provide more knowledge of necessary information of iris attributes are important [7].

4.1 Iris Feature Extraction and Recognition

The correlation is a way to measure how associated or related two variables are. The purpose of doing correlations is to make a prediction about one variable based on what know another variable. The proposed system uses the correlation method to identify whether the card holder is authentic or not. The human's iris looks like a circle. The circle has 360° in Cartesian coordinate. In this proposed system, firstly the iris is divided into 10 sectors. As the whole iris has 360°, each sector has 36°. The next step is to compare the pixel values from each sector. After matching pixel values for each sector, a relation becomes from these sectors. For example, the first sector's pixel values compare with the second sector's pixel values. The first sector has pixel value 7. The second sector has 14. The relation between these two sectors is 1:2. This relation is used as the feature extraction in this proposed system.
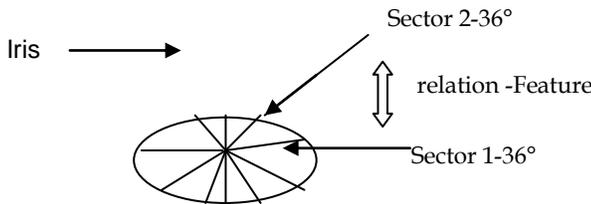

Figure2. Iris Feature Extraction of Proposed System
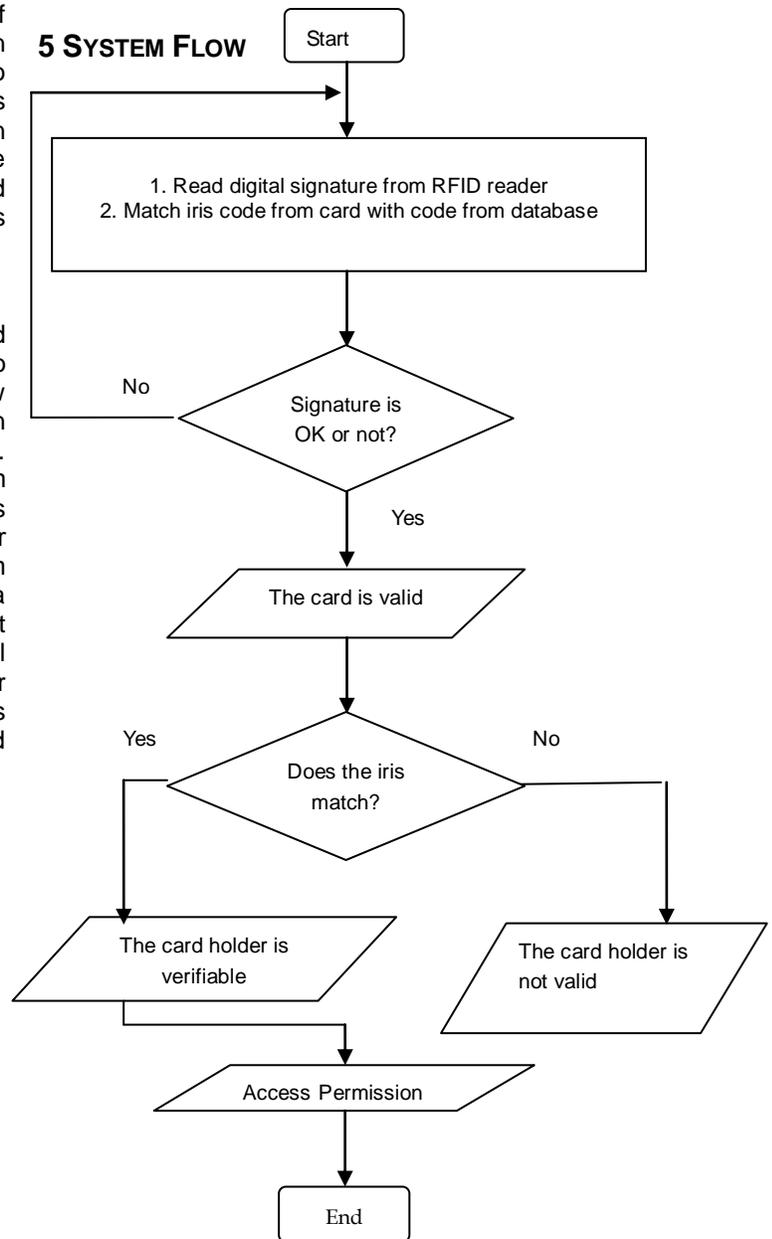
5 SYSTEM FLOW

Figure3. Block Diagram of Proposed System

The proposed system is the contactless personal identification system using cryptographic and biometric techniques with RFID. The major objective is to replace the paper-based identification system with digitized system. 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 production algorithm, a marking algorithm, and a validation algorithm. When the person comes in, the RFID reader reads the digital signature from the card. If the signature matches with the signature from the reader, 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. While implementing the proposed contactless id-card system, both the first module is that checking for person authentication performs with the combination of ECC (Elliptic Curve Cryptography) digital signature and RFID device. The second module is that testing for card validation carries out with new iris feature extraction using correlation method. The whole system is implemented with C#.Net programming language.

5 EXPECTED RESULTS

Nowadays, there are so many unauthorized card creation and unauthorized card holder reading when consuming the paper-based id-cards in the real world. The proposed system guarantees whether the person is either authentic or not. There is also able to give the security for data access control. The proposed system aims to prefer both the authorized card validation and authenticated card holder reading. And also the system intends to give more accurate and faster transaction time. The proposed system is able to set reliability, durability and convenience for users of contactless system.

6 SPECIFICATIONS AND LIMITATIONS

The proposed system has some preliminary data as input. First, the ECC digital signature must be assigned into the RFID card. Then the iris code must also be put into the RFID card. When the person who holds the contactless id-card comes in, the first step is to check the card validation. After passing the first step, the next step is the person authentication. The proposed system requires the hardware requirement and database requirement. For hardware requirements, RFID card with 1Mbyte and RFID reader (SDK reader) are needed. For database requirements, the proposed system uses the Chinese iris database.

7 CONCLUSION AND FUTURE WORKS

The proposed system is to develop the contactless digitized identification system utilizing the digital signature within RFID card and iris recognition with one new iris feature extraction and recognition method. The first role is that ECC digital signature is embedded into the RFID reader. The purpose of this role is to give card validation. The second role is that to implement new iris feature extraction and recognition using correlation method. The aim of this role is to ensure that the authenticated card holder only accesses the permission. Based on our findings, we intend to go into the next phase of the proposed system which is to develop the national security for long range and national registration system.

ACKNOWLEDGMENT

REFERENCES

[1] Ismarani Ismail and Mohammad Farid Saaid, *"Bus Detection Device for the blind using RFID application"*, IEEE, 2002.

[2] Patrik Fuhrer and Dominique Guinard, *"Building a Smart Hospital Using RFID Technologies"*, 2008

[3] Hind, John R, Mathewson, James M. II, Peters and Marcial, *"Identification and Tracking of Persons Using RFID-tagged items"*, November 7, 2002.

[4] Nandita Srivastava, *"Introduction, Present and Future applications and Security Implications"*, MSEE Student George Mason University, 2008.

[5] UPS Supply Chain, *"RFID in Healthcare",* white paper, 2005.

[6] Avi Kak, "*Lecture Notes on Computer and Network Security*", May 2, 2012.

[7] Tisse et al. *, Person identification technique using human iris recognition*