ISBN-978-989-53228-8-6
ISTANBUL XXIX International Conference on Research in “Science, Engineering and Technology” (IRSET-22)
Istanbul (Turkey) Mar. 21-23, 2022

Development of Input Control System Based on Contact ID Card Reading Technology

V. Gazieva and V. Tulyaganova[1]

[1] Tashkent University of Information Technologies, Department of Electronics and Radio Engineering, Uzbekistan

Abstract: *This article analyzes the development directions of the access control system based on contactless ID card reading technology. The advantages and disadvantages of using contactless ID cards are also analyzed. In addition, our study provides conclusions and recommendations for the development of an access control system based on contactless ID card reading technology. In addition, conclusions and recommendations on the development of input control system based on contact id card reading technology are given.*

Keywords: *contactless ID card, reading technology, RFID cards, vulnerability contactless cards.*

1. Introduction

Accelerated development of the information system in the country, the widespread use of modern information and communication technologies in the provision of public services, the introduction of a single mechanism of identification in various information systems and remote services, as well as the five priorities of the Republic of Uzbekistan in 2017-2021. The State Program on the implementation of the Action Strategy in the Year of Science, Enlightenment and Digital Economy has been identified as a separate task. An access card is a user ID that contains some information - a key that opens a door or access to resources. It is hard to imagine the modern world without contactless and contactless identification technologies. Use of bank cards (magnetic stripe, EMV chip cards, contactless payments PayPass, payWave); RFID cards for transport, entertainment and loyalty programs: issuance of compulsory health insurance policy and social cards of Moscow, and, of course, physical access and logical access cards to the computer and the company's IT resources. extensive use of access cards. However, “card” is a common concept because the identifier key can be in the form of a fob, a tag, a tag, and so on. Mobile phones or other devices that support NFC technology are not long in coming. used as an identifier.

Therefore, the issue of security of data transmission from the ID to the reader is more relevant than ever. The risk of copying data from cards and cloning them is increasing every day, which forces us to take a more conscious approach to the choice of technologies that provide secure identification. These are:

First, the vulnerability is typically assessed by three main threats identified when working with contactless cards: data privacy, duplication of access cards, and cloning.

Second, the unreliability of confidential information, if the identifier is stored in a clear form and is not protected from any reading, makes the access card and the entire system the most vulnerable, allowing attackers to access not only the object but also the data. about the cardholder. The problem is solved using

https://doi.org/10.17758/DIRPUB10.AE03221018

DES, 3DES, AES encryption algorithms. We have developed the following conclusions and recommendations for the development of an access control system based on contactless ID card reading technology:

- First, the Reading range, as well as the organization of use in a very wide range from 0 (contact access cards) to 300 meters (active contactless cards).
- Second, the two technologies are often used as additional protection on joint access cards, and the leading technology in this segment of ACS is undoubtedly the development of RIFD (Radio Frequency Identification) - a radio frequency identification system. allows quick access to the system without requiring the exact position of the tag. In addition, RIFD cards allow you to work in a harsh environment, perform long-distance identification, and have a long lifespan.

Preventing access of unauthorized person into restricted area in an electronically way, has been a vital approach to ensure that the security of an area is not compromised. A number of access control technique has evolved over time, each having its own merits and demerits. In biometrics method of access control, a person physiological and behavioral characteristic is extracted to perform person recognition. Among those characteristics are: fingerprint, hand geometry, handwriting, handprint, iris, palm vein, voice and retinal. These characteristics have been a subject of much research to provide human identification and access control functions. In [1], finger vein human identification system which can be used for access control was presented. Simple pattern matching method was used to reduce computation time for embedded environments, but the success rate is 97.6% and is therefore not suitable for personal security field. A finger vein and texture recognition technique based on repeated linetracking; Gabor filter and Neural Network was proposed in [2], though it may be cost effective and more accurate than some algorithm, long computation time will limit its usage. Palm vein authentication device that uses blood vessel patterns as a personal identify factor was presented in [3]. Although it has high level of accuracy, false acceptance and false rejection is still a problem. An Iris controlled door system was presented in [4], however costly image capturing equipment and long processing time is inherent in the system. Facial recognition and artificial neural network were combined to simulate a secure keyless door solution in [5].

2. Methods

A card reader is a data input device that reads data from a card-shaped storage medium. The first were punched card readers, which read the paper or cardboard punched cards that were used during the first several decades of the computer industry to store information and programs for computer systems. Modern card readers are electronic devices that can read plastic cards embedded with either a barcode, magnetic strip, computer chip or another storage medium. A smart card reader is an electronic device that reads smart cards and can be found in the following form [6]:

- Some keyboards have a built-in card reader.
- External devices and internal drive bay card reader devices exist for personal computers (PC).
- Some laptop models contain a built-in smart card reader and/or utilize flash upgradeable firmware.

External devices that can read a Personal identification number (PIN) or other information may also be connected to a keyboard (usually called "card readers with PIN pad"). This model works by supplying the integrated circuit on the smart card with electricity and communicating via protocols, thereby enabling the user to read and write to a fixed address on the card [7].

TABLE I: Communication protocols

Name	Description
T=0	Asynchronous half-duplex byte-level transmission protocol, defined in ISO/IEC 7816-3
T=1	Asynchronous half-duplex block-level transmission protocol, defined in ISO/IEC 7816-3.
T=2	Reserved for future use
T=3	Reserved for future use
Contactless	APDU transmission via contactless interface ISO/IEC 14443

If the card does not use any standard transmission protocol, but uses a custom/proprietary protocol, it has the communication protocol designation T=14.

The latest PC/SC CCID specifications define a new smart card framework. This framework works with USB devices with the specific device class 0x0B. Readers with this class do not need device drivers when used with PC/SC-compliant operating systems, because the operating system supplies the driver by default.

3. Analysis Of The Relevant Literature

3.1. Magnetic stripe

Magnetic stripe technology, usually called mag-stripe, is so named because of the stripe of magnetic oxide tape that is laminated on a card. There are three tracks of data on the magnetic stripe. Typically the data on each of the tracks follows a specific encoding standard, but it is possible to encode any format on any track. A mag-stripe card is cheap compared to other card technologies and is easy to program. The magnetic stripe holds more data than a barcode can in the same space. While a mag-stripe is more difficult to generate than a bar code, the technology for reading and encoding data on a mag-stripe is widespread and easy to acquire. Magnetic stripe technology is also susceptible to misreads, card wear, and data corruption. These cards are also susceptible to some forms of skimming where external devices are placed over the reader to intercept the data read [8].

3.2. Wiegand card

Wiegand card technology is a patented technology using embedded ferromagnetic wires strategically positioned to create a unique pattern that generates the identification number. Like magnetic stripe or barcode technology, this card must be swiped through a reader to be read. Unlike the other technologies, the identification media is embedded in the card and not susceptible to wear. This technology once gained popularity because it is difficult to duplicate, creating a high perception of security. This technology is being replaced by proximity cards, however, because of the limited source of supply, the relatively better tamper resistance of proximity readers, and the convenience of the touch-less functionality in proximity readers.

Proximity card readers are still referred to as "Wiegand output readers", but no longer use the Wiegand effect. Proximity technology retains the Wiegand upstream data so that the new readers are compatible with old systems.

3.3. Proximity card

A reader radiates a 1" to 20" electrical field around itself. Cards use a simple LC circuit. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil, which transmits it to the reader [9].

A common proximity format is 26-bit Wiegand. This format uses a facility code, sometimes also called a site code. The facility code is a unique number common to all of the cards in a particular set. The idea is that an organization will have their own facility code and a set of numbered cards incrementing from 1. Another organization has a different facility code and their card set also increments from 1. Thus, different organizations can have card sets with the same card numbers but since the facility codes differ, the cards only work at one organization. This idea worked early in the technology, but as there is no governing body controlling card numbers, different manufacturers can supply cards with identical facility codes and identical card numbers to different organizations. Thus, there may be duplicate cards that allow access to multiple facilities in one area. To counteract this problem some manufacturers have created formats beyond 26-bit Wiegand that they control and issue to organizations.

In the 26-bit Wiegand format, bit 1 is an even parity bit. Bits 2–9 are a facility code. Bits 10–25 are the card number. Bit 26 is an odd parity bit. 1/8/16/1. Other formats have a similar structure of a leading facility code followed by the card number and including parity bits for error checking, such as the 1/12/12/1 format used by some American access control companies [10]:

1/8/16/1 gives as facility code limit of 255 and 65535 card number

1/12/12/1 gives a facility code limit of 4095 and 4095 card number.

Wiegand was also stretched to 34 bits, 56 bits and many others.

3.4. Access Control Server

Every access control system needs a server where the permissions are stored in an access database. As such it acts as the center, or “brain,” of the access control system. It is really the server that makes the decision whether the door should unlock or not by matching the credential presented to the credentials authorized for that door. The server can be a dedicated local Windows or Linux computer, a cloud server, or even a decentralized server (when the permissions are stored in the door reader). The server also tracks and records activity and events regarding access, and it allows administrators to pull reports of past data events for a given time period.

If a locally-hosted access control server is used, there is typically a dedicated machine that runs the access software on it. Managing it requires the administrator to be on-site. Since having to contend with several local servers can become complicated for multi-facility management, cloud-based servers are gaining a lot of traction in this area.

4. Discussion Of The Results

In the form of credit cards and SIM cards, smart cards are the most common form of IT processing power on the planet.

It's is estimated that between 30 to 50B smart cards are in circulation today.

The smart card has a microprocessor or memory chip embedded in it with the processing power to serve many different applications when coupled with a smart card reader.

In the last three decades, these tools, more than any other technology, have quietly taken us all into a virtual world.

- Smart credit cards mediate daily transactions worth trillions of dollars.
- SIM cards facilitate billions of conversations that bind together our social and economic worlds.
- As an access-control device, smart cards (company badges, university IDs) make personal and business data available only to the appropriate users.

- As a National eID card, smart health card, residence permit, or electronic passport, smart card technology offers more robust identification and authentication tools for both authorities' and citizens' benefits.
- As a driver's license or a tachograph card, the technology contributes to road safety.

5. Acknowledgments

5.1. 2022-2023 market share forecasts:

1. Telecom (SIM cards) accounts for 52% of the total market,
2. Payment and banking cards for 34%,
3. Government (eIDs and e-passports) and healthcare for 4%,
4. Device manufacturers for 5%: mobile phones, tablets, navigation devices, and other connected devices, including an embedded secure element without SIM application,
5. Others for 5%: cards issued by operators, for transport, toll or car park services; cards for pay-TV; physical and logical access cards.

5.2. Electronic IDs

An electronic ID (e-ID) card fulfills various roles: it acts as a traditional means of identification, as a travel document, and finally, as a passkey to citizen's data.

Many international regulations and standards have been established on e-ID, most of which are applied by States.

The public has become accustomed to computerized smart cards through their use in the banking system, and as a result, their reliability is no longer questioned.

National ID cards are now also being used to access an array of services that were previously difficult to synchronize.

The e-ID card (aka computerized National identity cards) can be used for identification and authentication and electronic signature. Thus, this system enables several previously complex information paths to be simplified.

It can be used as:

- A representation of sovereign authority certifying that the holder is in a legitimate legal position to their national jurisdiction.
- A means for citizens to access services and exercise their rights and duties to the public authorities.
- A genuine seal of authenticity that the citizen can use to authenticate their actions regardless of the exchange formats and media used, since the data used to ensure security and trust also guarantee the legal validity of any transactions certified in this way.

There are markets for both disposable and reloadable cards. Disposable cards work well for an event and as a collectible card.

If the card is a multiple application card supporting, for example, debit and credit and stored value, the customer would not want to throw this type of card away. It would be more appropriate if the stored value application is reloadable. This process is sometimes called "post-issuance."

5.3. The Smart Card Alliance

The Smart Card Forum represents a diverse group of industries and government groups, many of whom have seemingly competing interests.

Today, even competing entities agree that where new technologies are concerned, industry-wide efforts are required to build workable infrastructures and to develop compatible, interoperable, multi-use systems. This effort cannot be accomplished, on any meaningful scale, by individual players acting in their own interests.

To date, the Forum has been highly successful in fostering communications across industries and the public sector and in encouraging various trials that demonstrate the viability of smart card-based payment and information systems.

Reference

[1] K.W. Ko, J. Lee, M. Ahmadi, and S. Lee, "Development of Human Identification System Based on Simple Finger Vein Pattern Matching Method for Embedded Environments," International Journal of Security and Its Applications, vol. 9, no. 5, pp. 297-306, 2015.

https://doi.org/10.14257/ijsia.2015.9.5.29

[2] R. Kaur and R. Rani, "An Identity Authentification Using Finger Vein and Texture Images Using NN," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 7, pp. 983-988, July 2014.

[3] I. Sarkar, Alisherov F., T. Kim, and D Bhattachayya, "Palm Vein Authentication System: A Review," International Journal of Control and Automation, vol. 3, no. 1, pp. 27-34, March 2010.

[4] "Mobile Credit Card Readers Grow with IOS as Foundation". Macworld.com. Retrieved March 22, 2012.

[5] ISO/IEC 7816-3:2006 Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols, clause 8.2.3

[6] "Bar Code Basics". Online Conveyor Parts. Archived from the original on January 16, 2012. Retrieved March 22, 2012.

[7] Dinora Baratova, Khayrullo Khasanov, Ikromjon Musakhonzoda, Shokhruh Abdumuratov and Khusniddin Uktamov. The impact of the coronavirus pandemic on the insurance market of Uzbekistan and ways to develop funded life insurance. E3S Web of Conferences 296, 06028 (2021)https://www.e3sconferences.org/articles/e3sconf/abs/2021/72/e3sconf_esmgt2021_06028/e3sconf_esmgt2021_06028.html

https://doi.org/10.1051/e3sconf/202129606028

[8] Uktamov Kh. F. and act. Improving the Use of Islamic Banking Services in Financing Investment Projects in Uzbekistan. REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS (Management, Innovation and Technologies) Journal. Vol. 11 No. 2 (2021). http://www.revistageintec.net/index.php/revista/article/view/1869.

https://doi.org/10.47059/revistageintec.v11i2.1869

[9] Akbarovich Yadgarov, A., Khotamov, I., Fakhriddinovich Uktamov, K., Fazliddinovich Mahmudov, M., Turgunovich Yuldashev, G. and Ravshanbek Dushamboevich, N. (2021). Prospects for the Development of Agricultural Insurance System. Alinteri Journal of Agriculture Sciences, 36(1): 602-608. doi: 10.47059/alinteri/V36I1/AJAS21085. http://alinteridergisi.com/article/prospects-for-the-development-of-agricultural-insurance-system

[10] Tukhtabaev, J.S., Rakhmonov, A.N., Uktamov, K.F., Umurzakova, N.M., & Ilxomovich, R. (2021). Econometric Assessment of Labor Productivity in Ensuring the Economic Security of Industrial Enterprises. International Journal of Modern Agriculture, 10(1), 971-980. http://modern-journals.com/index.php/ijma/article/view/700