# AN EFFIFICIENT AUTHENTICATION AND ACCESS CONTROL SCHEME USING SMART CARD

Dhanashree R. Landge[1], Pushkaraj S. Jadhav[2], S. C. Rajgade[3]
[1,2]Final Year Student, [3]Assistant Professor and Research Scholar
Department of Instrumentation and Control, AISSMS Institute of Information Technology
Pune, India

***Abstract: In modern society, computer systems are in widespread use to store resources. With the well development of network technologies a recent trend in computer systems is to store various resources in distributed computer systems. As a result, these resources may be shared through the network in the form of network services provided by servers. To provide these resources to only identified users is quite important. Thus, in order to protect these resources from being unauthorized accessed, both user authentication and access control are required for resource protection in distributed computer systems. Here we have proposed the access control scheme at a software company to provide the protection among eight doors. It will allow only authorized users to access into eight various sections of an office.***

***Index Terms: Door Access Control System, Smart Card, Authentication, Security.***

## I. INTRODUCTION

Managing access to resources is assuming increasing importance for organizations everywhere, from small entrepreneurial companies to large corporate enterprises and government bodies of all sizes. Even the most neutral organization now recognizes the danger of a security breach. Administering access to resources means controlling both physical access and logical access, either as independent efforts or through an integrated approach. Physical access control protects both tangible and intellectual assets from theft or comprises. Logical access control enables enterprises and organizations to limit access to data, networks and workstations to those authorized to have such access. Coordinating people and privileges has traditionally relied on the use of an identity card such as driver's license, library card, credit card, membership card or employee identification card. Such cards verify to a person or a device that the holder has particular rights and privileges. In response to the need for increased security, industry developed technologies (such as magnetic stripe, bar codes and proximity chips) that can be included on a card. The card can then be passed through a magnetic stripe reader, scanned by a bar code reader, or presented to an electronic reader with an RF antenna for automatic access authorization. A personal identification number (PIN) can be entered via a keypad to add another authentication factor to help verify that the cardholder is indeed the owner of the card. However, while these technologies reduce cost and increase convenience, they do not guarantee that the user is in fact the authorized person.

Smart card based physical access control systems are powerful and efficient security tool for protecting enterprise assets. Each employee or contractor is issued a smart ID card displaying enterprise information and printed designs, both to thwart the possibility of counterfeiting and to identify the card as official. Each card stores protected information about the person and the person's privileges. When the person is initially enrolled and accepts the card, these privileges are accurately and securely populated throughout the system. When the card is placed in or near an electronic reader, access is securely and accurately granted or denied to all appropriate spaces (e.g a campus, a parking garage, a particular building, or an office). When an employee leaves an organization, all physical access privileges are removed once. Any future attempt by that person to re-enter the premises using an expired or revoked card could be denied and recorded automatically.

### *A. SYSTEM DESIGN*

To the user, an access control system is composed of three elements:

- A card or token (an identity credential) that is presented to door reader
- A door reader, which indicates whether the card is valid and entry is authorized
- A door or gate, which is unlocked when entry is authorized

Behind the scenes is a complex network of data, computers, and software that incorporates robust security functionality. It provides a context for understanding how contact and contactless smart card technologies are used in an access control application.

A typical access control system is made up of the following components:

1. ID credential (Smart Card)
2. Door reader (Smart card reader)
3. Door Lock
4. Control Panel
5. Access control server
6. Software
7. Database

  

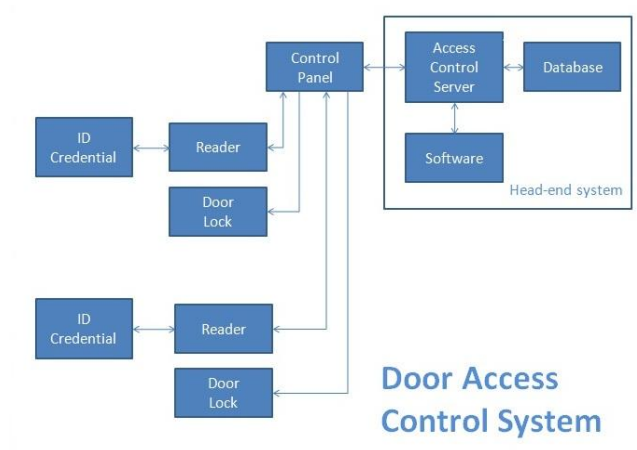


Fig. 1: Block Diagram

*1. ID Credential (Smart Card)*

A number of different ID technologies are currently in use for access control: Magnetic strips, Wiegand strips, barium ferrite, and 125 kHz proximity technology, contact smart card and contactless smart cards. However, all credentials operate in basically the same way: they hold data that authenticate the credential and/or user. Some credential technologies are read-only. Information is permanently recorded on the credential, and when the credential is presented to a reader, the information is sent to the system. This type of credential only validates that the information itself is authentic. Credentials that use these technologies are intelligent devices. They can store privileges, authorizations, and attendance records. They can store PINs and biometric templates, offering two-or-three factor authentication capability. The credential is no longer just a unique number holder, but is a secure, portable data carrier as well.

*2. Door Reader (Smart card reader)*

When the reader has received all required data, it typically processes the information in one of two ways. Either the information is immediately sent to the control panel, or the reader analyzes the data before sending it to the control panel. Readers that analyze data must be integrated into the access control system. That is, they must interpret and manipulate the data sent by the card and then transmit the data in a form that is usable by the control panel. The process of authenticating the card to the reader and the reader to the card is called mutual authentication.

*3. Control Panel*

The control panel (often referred to as the controller or simply the panel ) is the central communications point for the access control system. It typically supplies power to and interfaces with multiple readers at different access points. The controller connects to the electro-mechanical door lock required to physically unlock a door or to the unlocking mechanism for an entrance portal. The control panel makes the decision to unlock the door and passes the transaction data to the host computer and unlocking signal to the reader. It is important for the control panel is located inside the facility or in a secure room, while the card reader is located in an insecure or open area. The control panel stores data format information. This information identifies what portion of the data stream received from a card is used to make access control decisions.

Fig. 2: Control Panel

*4. The Access Control Server*

The head-end system includes the access control server, software, and a database. The database contains updated information on user's access rights. The access control server receives the card data from the control panel. The software correlates the card data with data in the database, determines the person's access privileges, and indicates whether the person can be admitted.

*5. Access Control System Data Formats*

The access control system's data format in a critical design element. Data format refers to the bit pattern that the reader transmits to the control panel. The format specifies how many bits make up the data stream and what these bits represent. For example, the first few bits might represent the facility code, the next few a unique credential ID number, the next few parity, and so on.

## II. WORKINF OF A PROJECT

The access control process begins when a user presents the credential to the reader, which is usually mounted next to a door or entrance portal. The reader extracts data from the card, processes it, and sends it to the control panel. The control panel first validates the reader and then accepts the data transmitted by the reader. The control panel transmits the data to the access control server. The access control server compares the data received from the card with information about the user that is stored in a database. Access control software determines the user's access privileges and authorization, the time, date, and door entered, and any other information that a company may require to ensure security. When access is authorized, the access control server sends a signal to the control panel to unlock the door. The control panel then sends out two signals: one to the appropriate door lock, which unlocks the door, and one to

  

the door reader, which emits an audible sound or otherwise signals the user to enter.

## III. CONCLUSION

This project is performed to define the long-term objectives for a new physical access ID system and develop a careful migration strategy and plan that implements the system in a logical, convenient, timely and cost-effective way. Migrating to a newer access control technology can be economical and relatively straightforward if the move is well planned.

## REFERENCES

[1] B.G. Liptak, "Process Measurement And Analysis", 3rd ed. vol. 1, Chilton Book Company, Radnor, Pennsylvania.
[2] Raul Sanchez-Reillo, "Fingerprint Verification Using Smart Cards for Access Control Systems", IEEE AES Systems Magazine, September 2002 .
[3] Narn-Yih Lee, "Integrating Access Control With User Authentication Using Smart Cards", IEEE Transactions on Consumer Electronics, Vol. 46, No. 4,November 2000
[4] Rand Sanchez-Rclllo and Ana Gonznlez-Marcas, "Access Control System with Hand Geometry Verification and Smart Cards", IEEE AES Systems Magazine, February 2000.

  