

A REVIEW OF TRENDS OF AUTHENTICATION MECHANISMS FOR ACCESS CONTROL

Adegun A.A.

Computer Science Programme
Landmark University
Omu-aran, Nigeria
adegun.adekanmi@lmu.edu.ng

Adigun A. A.

Department of Computer Science and Engineering
Ladoke Akintola University of Technology
Ogbomosho, Nigeria

Asani E.O.

Computer Science Programme
Landmark University
Omu-aran, Nigeria
asani.emmanuel@lmu.edu.ng
2348025717404

ABSTRACT

This work is a comprehensive overview of trends of authentication mechanisms for access control. It elaborates on different classes of authentication mechanisms such as PINs, Passwords, Smartcards and Biometrics, their uses and decryption. These authentication technologies are used to protect vital information as well as prevent unauthorized accessing of physical and logical resources in all information technology system. Of the entire authentication mechanisms worked upon, biometric is the most effective method of authentication, but it is very expensive to configure and maintain.

Keywords: PINs, Passwords, Smartcards and Biometrics

1. INTRODUCTION

Access control is a system that enables an authority to control access to areas and resources in a given physical facility or computer based information (Dan Goodin, 2008). It refers to exerting control over who can interact with the resource; sometimes it involves an authority that does the controlling. The resource can sometimes be computer based information. Access control is in reality of our everyday activities such as; the pin on an ATM system at a bank is a means of access control. The possession of access control is of prime importance when people seek to secure important, confidential or sensitive information and equipment(s). Before allowing an entity or entities to access a network and its associated resources, the general mechanism is to authenticate the entity (a device/or user) and then allow authorization based on the identity (cisco press, 2005). A computer system that is supposed to be used only by those authorized must attempt to detect and exclude the unauthorized. Access to it is therefore usually controlled by insisting on an authentication procedure to establish with some degree of confidence of the identity of the user, granting privileges established for that identity. The most common access control is binary; it either allows access or denies access based on membership in a group. Common examples of access control involving authentication include; asking for photo ID when a contractor first arrives at a house to perform work, logging into a computer, entering a country with a passport.

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artefact, or ensuring that a product is what its packaging and labelling claims to be (Ahmed & Jensen, 2009). The desire for property right and the ability to keep one's possession to one's self (or those to whom usage privileges have been extended) since ancient times, the desire to authenticate someone has become imperative in every facet of computer because the security is paramount in computing.

2. LITERATURE REVIEW & CONCEPTUAL UNDERSTANDING

2.1 Physical and Logical Access Control Convergence

Access control is a system that enables an authority to control access to areas and resources in a given physical facility or computer based information (Dan Goodin, 2008). Physical access control may be sufficient in environments where all users of a system need access to all of the information on it. In environments where not all information resources on a system should be equally available to all users, a more precise control is necessary.

Logical access control enhances the security provided by physical access control by acting as an additional guard against unauthorized access to or use of system's resources. It can also augment physical access control by providing added precision, since different users are able to perform different functions (Caelli et al, 2001).

As logical and physical access control begin to converge, the ability to identify individuals within an organization has become critically important. The requirements for a holistic security solution and the adoption of new access control technologies are driving dramatic and necessary changes both security measures. The most secure means of ensuring successful convergence of physical and logical access control is through integrated biometric application. Through fingerprint-based biometric technology, the problems of both unauthorized physical and logical access can be negated through a single technology.

2.2 Origin of Authentication

Passwords and personal identification numbers (PINs) have been used since ancient times. Passwords have been used with computers since the earliest days of computing. Biometrics can be traced to 14th century in China. The explorer Joao de Barros recorded that Chinese merchant were stamping children palm prints and footprints on paper with ink to distinguish the young children from one another. The practice is apparently still in use in some parts of the world. Bertillonage prompted Richard Henry of Scotland to seek a more reliable method of identifying criminals. Henry decided that finger printing was the most accurate way to do this, and the police began to adopt this as the primary method of criminal identification in the early 20th Century. Although finger printing is still in use today, computer aided techniques began developing rapidly in the last quarter of the twentieth century. These techniques sought to measure our voices, our hands, fingers, irises and faces. Once ideas were proposed, development was rapid (Galton & Francis, 1998).

2.3 Types of authentication mechanisms

2.3.1 A personal identification number (PIN)

It is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Typically, the user is required to provide a non-confidential user identifier or token (such as a banking card) and a confidential PIN to gain access to the system. Upon receiving the User ID and PIN, the system looks up the PIN based upon the User ID and compares the looked-up PIN with the received PIN. The user is granted access only when the number entered matches with the number stored in the system (Wikipedia, 2010). PINs are most often used for ATMs but are increasingly used at the point of sale, especially for debit cards. Throughout Europe the traditional in-store credit card signing process is being replaced with a system where the customer is asked to enter their PIN instead of signing. Apart from financial uses, Global Systems for Mobile Communication (GSM) mobile phones usually allow the user to enter PIN between 4 and 8 digits length. The PIN is recorded in the Subscriber Identity Module (SIM) card (Wikipedia, 2010).

2.3.1.1 PIN Length

The concept of a PIN originates with the inventor of the ATM, John Shepherd-Barron. One day in 1967, while thinking about more efficient ways banks could disburse cash to their customers, it occurred to him that the candy vending machine model was a proven fit. For authentication Shepherd-Barron at first envisioned a six-digit numeric code, given what he could remember. His wife however preferred four digits, which became the standard.

2.3.2 Password

A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (Fred Cohen et al, 2012). Most accounts on a computer system usually have some methods of restricting access to them, usually in form of a password. When accessing the system, the user has to present a valid identity (ID), followed by a password to use the account. A password should be kept secret, people wishing to gain access as tested on whether or not they know the password and are granted or denied access accordingly. They are generally short enough to be memorized. There is no need for it to be actual words, indeed passwords which are not words are harder to decode, but are generally harder for users to remember. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword. Sentries would only allow a person or group to pass if they knew the password. In recent times (modern), user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, automated teller machines (ATMs) etc. A typical computer user may require passwords for many purposes such as logging in to computer accounts, retrieving email from servers, accessing files, database, networks, and websites and even reading the morning newspaper online (Morris et al, 2012).

2.3.3 Smart cards

A smart card, chip card, or integrated circuit card (ICC), is defined as any pocket-sized card with embedded integrated circuits which can process information (smartcard alliance, 2009). This implies that it can receive input which is processed by way of the ICC applications-and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components. Smart cards are made of plastic, generally polyvinyl chloride (PVC), but sometimes acrylonitrile butadiene styrene (ABS) (Rankl, W & W. Effing, 2001). Smart card has been described as the "key to the global village" it is like an electronic wallet. It is a standard credit card sized plastic intelligent token within which a microchip has been embedded in which makes it "smart". The microchip is capable of processing data, providing memory capacity, and computational capability.

It has a gold contact that allows other devices to communicate with it. However, the marriage between a convenient plastic card and a microprocessor in a smart card allows information to be stored, accessed and processed either online or offline. The processing power of smart cards gives them the versatility needed to make payments, to configure your cell phones and connect to your computers via satellite or the internet (Guthery & Scott, 2001).

2.3.4 Biometrics

Biometrics is an old Greek word for a very new concept. “Bio,” meaning life, and “Metric,” the measure of, so biometrics is in essence, the measure of life (Allan et al, 2003). Biometric measures biological characteristics for identification or verification purposes of an individual. Since IDs and passports can be forged, more sophisticated methods are needed to be in place to help protect companies and individuals. In biometry, there are two types of biometric methods. One is called behavioural biometrics; it is used for verification purposes. Verification involves confirming or denying a person’s claimed identity. This method looks at pattern of how certain activities are performed by an individual (Jain et al, 2007). Physical biometrics is the other type used for identification or verification purposes. Identification establishes a person’s identity. This method is commonly used in criminal investigations (Sheila Robinson, 2011).

Biometrics provides a better solution for the increased security requirements of our information society than current identification methods (passwords, PIN numbers and magnetic strip cards with a PIN number) for various reasons: the person to be identified must be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password (or write it on a yellow sticky note), PIN or carry a token. Using biometric systems to identify the user of a computer, ATM, cellular phones and even credit card purchases will reduce fraud and unauthorized access. This could save the economy billions of dollars.

2.3.4.1 Some biometric technologies

Fingerprint identification

Fingerprint identification is the most commonly recognized and most widely applied form of biometric technology. Fingerprint ID is based upon the fact that a person’s fingerprint is completely unique to the individual. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points (Vokey et al, 2009). In the past, fingerprints were recorded by the application of ink to the finger which was then pressed to paper to give an impression. More recently, it has become possible to scan a person’s fingerprint into virtual storage in a computer with the aid of laser technology. In order to prove identification, a person’s fingerprint will be scanned again in the future by a similar device, and a match of print to name is verified through information systems. Fingerprint scanning secure entry devices for building door locks. Also, a small number of banks have begun using fingerprint readers for authorization at ATMs and grocery stores are experimenting with a fingerprint scan checkout that automatically recognizes and bills a registered user’s credit card or debit account.

Hand geometry

Hand geometry is even older than digital fingerprinting; it was first used for security purposes on the American Wall Street more than twenty years ago. Hand geometry is based on the fact that virtually every person’s hand is shaped differently and that the shape of a person’s hand (after a certain age) does not significantly change. When the user places a hand on the hand reader, a three-dimensional image of the hand is captured. Then, the shape and length of the fingers and knuckles are measured. Depending on the data used to identify a person, hand reading technologies generally fall into one of three categories-applications to the palm, the pattern of veins in the hand and the geometrical analysis of fingers (Matt Spencer, 2001).

Eye scanning

Biometrics which analyzes the complex and unique characteristics of the eye can be divided into two different fields: iris biometrics and retina biometrics. The iris is the colour band of issue that surrounds the pupil of the eye. Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of an individual’s eyes, whose complex random patterns are unique and can be seen from some distance (Daugman & John, 2004). The retina is the layer of blood vessels at the back of the eye. A retinal scan is a biometric technique that uses the unique patterns on a person’s retina to identify those (Hill & Robert, 2007). Retina scans are performed by directing a low-intensity infrared light to capture the unique retina characteristics. An area known as the fovea, situated at the center of the retina, is scanned and the unique pattern of the blood vessels is captured. Retina biometrics is considered to be best biometric performers. However, despite its accuracy, this technique is often thought to be inconvenient and intrusive. And so, it is difficult to gain general acceptance by the end user. The retinal scanner requires an individual to stand while it is reading the retinal information. Eye and retinal scanner are ineffectual with the blind and those who have cataracts.

Face recognition

Face recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source (Smith & Kelly, 2008). The system identifies an individual by analyzing the unique shape, pattern and positioning of facial features. There are essentially two methods of processing the data: video and thermal imaging. Standard video techniques are based on the facial image captured by a video camera. Thermal imaging techniques analyze the heat-generated pattern of blood vessels underneath the skin. The attraction of this biometric system is that it is able to operate ‘hands free’, limiting the amount of man-machine interaction. However, this system is highly unreliable and expensive.

For example, it will not distinguish twins or triplets, it will not recognize the user after a haircut, and it may not recognize a person who changes from wearing and not wearing glasses. As concerns face recognition, many approaches have been proposed in the literature, and several researchers are studying this problem. Principal component analysis, elastic graph matching, neural networks, and distortion-tolerant template matching are only few of the proposed techniques.

DNA

The term “DNA” means deoxyribonucleic Acid. DNA is found in every cell of every creature, and it contains the information for carrying out the activities of the cell. Since every person’s DNA structure is completely unique, DNA analysis is a very accurate way of proving identification. Due to the extensive testing and advanced technology required, it is not the most cost efficient biometric science, but when a positive identification is needed it is the most reliable (Pbworks, 2006).

Other future applications.

Biometric based authentication applications include work-station and network access, single sign-on or application logon, data protection, remote access to resources, transaction security and web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, health and social services are already benefitting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large scale enterprise network authentication environment, point of sale, and for the protection of all types of digital content applications utilized alone, or integrated with other technologies such as smartcards, encryption keys, and digital signatures. Biometrics is anticipated pervade nearly all aspect of the economy and our daily lives (Debnath Bhattacharyya et al, 2009).

2.4 Authentication Security Systems

Security is used frequently, but the content of a computer is exposed to little risks unless the computer is used by others or connected to other computer systems on the network. As the use of computer system has become persistent, the concept of computer security has expanded to denote issues pertaining to use of computer and their resources. Often, traditional computer security system require the user (s) to provide a username and password to gain access to a protected computer system, while modern computer system use smart cards or other security tokens to authenticate computer users. Both the use of password and token-based systems are prone to security risk by unauthorized users; for example, most password are recorded on or near the computer that they’re intended to secure and if an individual’s contactless smart card is stolen, anyone can use it. Computer hijackers have been able to write some software which can be used to crack username and password.

The major technical areas of computer security are usually represented by confidentiality, authentication and integrity. Confidentiality is known as privacy of a computer system from other users, integrity means that information is protected against unauthorized changes that are not detectable to authorized users and availability means that resources are accessible by authorized parties (Winer, 2003). Other important computer security concerns are access control and non-repudiation. Maintain access control means not only that user can access only those resources and services to which they are entitled to, but also that they are denied resources that they legitimately can expect to access. Non-repudiation implies that a person who sends a message cannot deny not sending it and, conversely, that a person who has received a message cannot deny not receiving it.

In addition to these technical aspects, the conceptual reach of computer security is broad and multifaceted. Computer security is concerned with topics such as computer crime; the prevention, detection, and remediation of attacks; and anonymity in cyberspace (Winer, 2003). Previously, Password was the primary means of authenticating computer users. Nowadays, system administrators are becoming concerned about the limited security provided by password and username authentication. Many system administrators are now concluding that their password based computer security systems are not all that secured. User passwords are routinely stolen, forgotten, shared, or intercepted by hackers. Another serious problem is that computer users have become too trusting. They routinely use the same password to enter both secure and insecure Web sites as well as their networks at work.

In response to the proven lack of security provided by password authentication, network administrators are replacing network passwords with smartcards, biometric authentication, or a combination of the three. Smart cards are credit card-size devices that generate random numbers about every minute, in sync with counterparts on each entry point in the network. Smart cards work well as long as the card isn’t stolen. A better choice to ensure network security is the use of biometrics. Biometric-base authentication and identification methods are emerging as most reliable.

2.5 Characteristics of Authentication Systems.

Biometrics systems are essentially nothing-to-remember systems and they are always carried with the individual. Biometrics systems are low cost, faster and accurate; easiest of all authentication systems, the basic abilities of a cryptographic system is to maintain the integrity and confidentiality of data. Smart card systems are portable for identification credentials, they reduce tampering and counterfeiting through high security mechanisms, such as advanced encryption and biometrics, and they are reusable or disposable and perform multiple functions. The amount of security and inconvenience inherent in a particular password system policy are affected by several factors such as allowable inputs, minimum and maximum time required for input, error tolerance etc. Some password protected systems pose little or no risk to a user if compromised. Some passwords pose modest economic or privacy risk and they could have very serious consequences if compromised.

2.6 Areas of application of authentication mechanisms

1. **Health care (for privacy of medical records):** both smart cards and biometrics are used in identity management systems to verify individual's identities. Biometrics alone, smartcards alone, and a combination of smartcards with biometrics are options for health care organizations moving to stronger, electronic identity authentication of patients and providers. Smartcard technology provides a strong foundation for health ID cards, enabling improvement in health care processes and in patient and provider identity verification, while securing information and protecting privacy (smartcard alliance, 2012).
2. **Physical access control (government agencies):** The E- authentication initiative (EAI) was established to assist agencies in their efforts to develop trust relationships with their user communities through the use of electronic identity credentials. It is an identification standard for federal employees and contractors who are conducting business with federal agencies and who require access to physical and information technology resources. The EAI provides the capability for any government agency to validate an electronic identity credentials to authenticate an individual's identity before that individual is granted access to IT or physical resources (smartcard alliance, 2009).
3. **Financial services (internet banking):** the specific nature of internet banking systems creates the requirement of specialized knowledge on security issues to be able to effectively conduct an auditing or security evaluation process (Christos, 2007).
4. **Telecommunications (mobile phones, call centre technology):** passwords and PINs are often used in mobile phones as a means of verifying the authenticity of the person operating the mobile phone. Service providers usually provide a subscriber with a PUK number when he/she purchases a new SIM card for authentication purposes.

3. DETAILED ANALYSIS OF AUTHENTICATION MECHANISMS

3.1 Personal Identification Number

Financial PINS are often 4-digits numbers in the range 0000-9999, resulting in 10,000 possible numbers. However, some banks do not give out numbers where all digits are identical (such as 1111, 2222 ...) or consecutive (1234, 2345 ...) or numbers that start with one or more zeroes. Many PIN verification systems allow three attempts, thereby giving a card thief a 3/10000 chance to guess the correct PIN therefore the card is blocked. This holds only if all PINs are equally likely and the attacker has no further information available, which has not been the case with some of the many PIN generation and verification algorithms that banks have used in the past. If a mobile phone PIN is entered incorrectly three times, the SIM card is blocked until a Personal Unblocking Code (PUC) is provided by the service operator is entered. If the PUC is entered incorrectly ten times, the SIM card is permanently blocked, requiring a new SIM card (Pedssoftware, 2012).

3.1.1 Mode of operation

A typical example of how PIN works is illustrated on an ATM machine. When someone is short of cash, he/she walks over to the automated teller machine (ATM), insert his/her card into the card reader then respond to the prompts on the screen and within some seconds he/she walks away with cash and a receipt. These machines can also be found in most standard supermarkets, conveniences stores and travel centres. PIN is a unique personal password that you punch into an ATM or website to provide verification to the system that one is who you claimed to be and should have access to the system (John, 2010). Any ATM machine needs a data terminal with two inputs and four output devices. For this to happen there should also be the availability of a host processor. The host processor is necessary so that the ATM can connect and also communicate with the person requesting the cash. The internet service provider (ISP) also plays an important role in this action. They act as the gateway to the intermediate networks and also the bank computer.

A leased-line ATM machine has a four-wire, point to point dedicated telephone line which helps in connecting with the host processor. Dial-up ATM machine connect to the host processor through a normal phone line using a modem and a toll-free number, or through an internet service provider using a local access number dialled by modem (John, 2010).

Leased-line ATMs are preferred for very high-volume locations because of their thru-put capability and dial-up ATMs are preferred for retail merchant locations where cost is a greater factor than thru-put. The initial cost for a dial-up machine is less than half that for a leased-line machine. The monthly operating cost for dial-up is only a fraction of the costs for leased-line.

3.1.2 Uses of personal identification number

It is mostly used on ATM or debit card identification and security. In Europe the traditional in-store credit card signing process is being replaced with a system where the customer is asked to enter their PIN instead of signing while in the United Kingdom and Ireland this goes under the term 'Chip and PIN'. Apart from financial uses, global system for mobile communications (GSM) phones usually allow the user to enter PIN between four to eight digit length, which is recorded in the Subscriber identity module (SIM) card.

3.2 Password

Most accounts on a computer system usually have some method of restricting access to that account, usually in the form of a password. When accessing the system, the user has to present a valid ID to use the system, followed by a password to use the account. Most systems either do not echo the password back on the screen as it is typed, or they print an asterisk in place of the real character. To crack a password requires getting a copy of the one-way hash stored on the server, and then using the algorithm generate your own hash until you get a match. When you get a match, whatever, word you sued to generate your hash will allow you to log into that system. Since this can be rather time-consuming, automation is typically used. There are freeware password crackers available for NT, Netware, and UNIX.

The best method of preventing password cracking is to ensure that attackers cannot get access even to the encrypted password. For example, on the Unix Operating System, encrypted passwords were originally stored in a publicly accessible file. On modern UNIX, (and similar) systems, on the other hand, they are stored in the file which is accessible only to programs running with enhanced privileges (i.e., 'system' privileges). This makes it harder for a malicious user to obtain the encrypted passwords in the first instance. Unfortunately, many common network protocols transmit the hashed passwords to allow remote authentication (Pedsoftware, 2012).

On most systems, the password is typically run through some type of algorithm to generate a hash. The hash is usually more than a scramble version of the original text that made up the password; it is usually a one way hash. The one way hash is a string of characteristics that cannot be reversed into its original text. You see, most systems do not decrypt the stored password during authentications; they store the one way hash. During the login process, you supply an account and password. The password is run through an algorithm that generates a one way hash; this hash is compared to the hash stored on the system. If they are the same, it is assumed the proper password was supplied. Cryptographically speaking, some algorithms are better than others at generating a one way hash. The main operating systems we are covering here – NT, Networks and UNIX - all use an algorithm that has been made publicly available and has been scrutinized to some degree.

3.3 Smart cards

Smart cards are about the same size as a credit card. Some vendors offer smart cards that perform both the function of a proximity card and network authentication. Users can authenticate into the building via proximity detection and then insert the card into their PC to produce network login credentials. They can also serve as ID badges. The downside is that the smart card is a bigger device; the card reader is an extra expense. A smart card, a type of clip card is a plastic card embedded with a computer chip that stores and transacts data between users. This data is associated with either value or information or both and is stored and processed within the card's chip, either a memory or microprocessor. The card data is transacted via a reader that is part of a computing system. Smart card-enhanced systems are in use today.

A smart card is a credit card-sized piece of plastic. It may even be a credit card. What makes a smart card different from any old piece of plastic and from magnetic – stripe cards is an embedded microchip. This microchip can be a microprocessor or simply a memory chip. While not making the card smarter than any other piece of plastic, the memory chip does increase the card's utility. A microprocessor card contains a small computer, as the name implies, complete with I/O port, storage and operating system (Smartcardbasic, 2012).

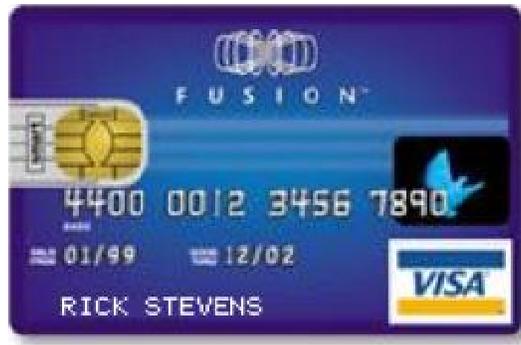


Figure 1 A smartcard (Smartcardbasic, 2012).

Microprocessor smart cards are small plastic cards embedded with a programmable microprocessor chip. They are tools for immediate and secure off-line access to essential information stored on the card (important linkage capabilities). They are inexpensive and secure means for on-line data access and transfer.

3.3.1 Mode of operation

Credit card can work both financially and technically. A credit card is a thin plastic card, usually 3-1/8 inches by 2-1/8 inches in size. It contains identification information such as a signature or picture, charges and authorizes the person's name on it to charge purchases or services to his account, charges for which he will be billed periodically. Today, the information on the card is read by automated teller machines (ATMs), stored readers and bank and internet computers. The stripe on the back of a credit card is a magnetic stripe, often called a mag-stripe. The mag-stripe is made up of tiny magnetic particles in a plastic-like film. Each particle is really a tiny bar magnet about 20-millionths of an inch long. The mag-stripe can be written because the tiny bar magnets can be magnetized in either in a north or South Pole direction. The mag-stripe on the back of the card is very similar to a piece of cassette tape (Gache, 2008).

Reader driver

Is a specific driver that maps driver services to a specific hardware reader device. It must communicate card insertion and removal event to the smartcard class driver in forwarding to the smartcard resource manager, and it must provide data exchange capabilities to the card.

Reader helper driver

It provides common smartcard driver support routines and additional protocol support to a specific driver that is needed.

Reader

It is a standard device between the smartcard subsystems. An interface device (IFD) that supports bidirectional inputs/outputs to a smartcard. It may be associated with an entire system, one or more reader groups, or with a specific terminal. The smartcard subsystem allows a reader to be dedicated to the terminal to which it is assigned.

Resource manager

It is the module of the smartcard subsystem that manages access to multiple readers and smartcards. A resource manager identifies and tracks resources, allocate readers and resources across multiple applications, and supports transaction primitives for accessing services available on a given card.

User

A user of a system is identified by a login procedure which establishes a process by which applications can run and access other security relevant objects. An example of login procedure is to use a smartcard, possibly in conjunction with a password or personal identification number (PIN).

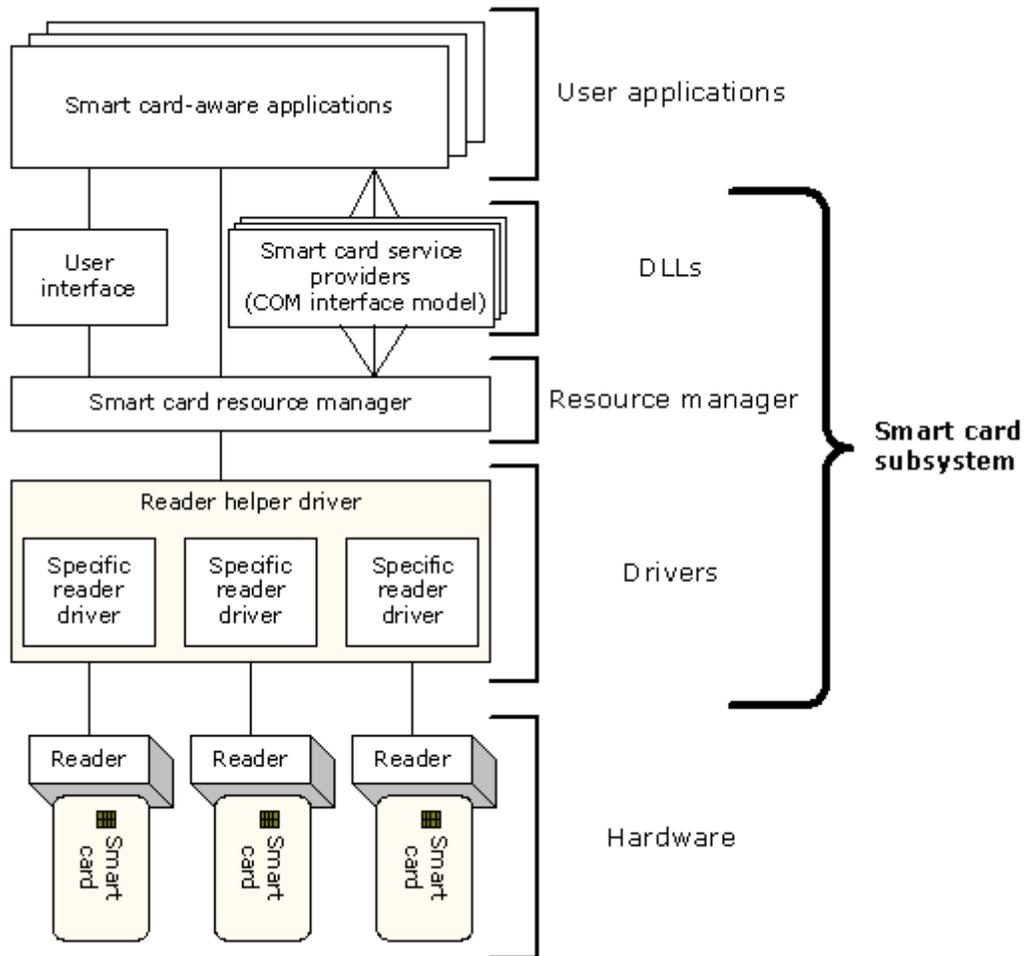


Figure 2: A block diagram of a smartcard (Windows development center, 2012).

User interface

It is a common dialog box that lets the user connect to a smartcard and use it in an application. Using the dialog box, the user can specify a specific card or search for the smartcard to open.

Service provider

A smartcard subsystem component that provides access to specific smartcard services by means of COM interfaces (windows development centre, 2012). A mag-stripe reader can understand the information on the three track stripe. If the ATM is not accepting your card, your problem is probably either;

- A dirty or scratched mag-stripe
- An erased mag-stripe (the most common causes for erased mag-stripe are exposure to magnets, like the small ones used to hold notes and pictures on the refrigerator, and exposure to a store's electronic article surveillance).

There are three tracks on the mag stripe. Each track is about one-tenth of an inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 per inch (bpi), and holds 79 6-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 4-bit plus parity bit characters
- Track three is 210bpi, and holds 107 4-bit plus parity bit characters.

Credit card typically uses only tracks one and two. Track three is a read/write track (which includes an encrypted PIN, country code, currency units and amount authorized), but its usage is not standardize among banks. This is how it works: after you or the cashier swipes your credit card through a reader, the EDC software at the point-of-sale (POS) terminal dials a stored telephone number (using a modem) to call an acquirer. An acquirer is an organization that collects credit authentications requests from merchants and provides the merchants with a payments guarantee. When the acquirer company gets the credit card authentication request, it checks the transaction for validity and the record on the mag-stripe for:

- Merchant ID
- Valid card number
- Expiration date
- Credit card limit
- Card usage

Single dial-up transaction is processed at 1,200 to 2,400 bits per second (bps), while a direct internet attachment uses much higher speeds via this protocol. In the system, the cardholder enters a personal identification number (PIN) using a keyboard.

3.4 Biometrics

Biometrics is the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). For common use, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioural characteristics, such as fingerprints, irises, voice patterns, facial patterns, and hand measurements, for identification and verification purposes.

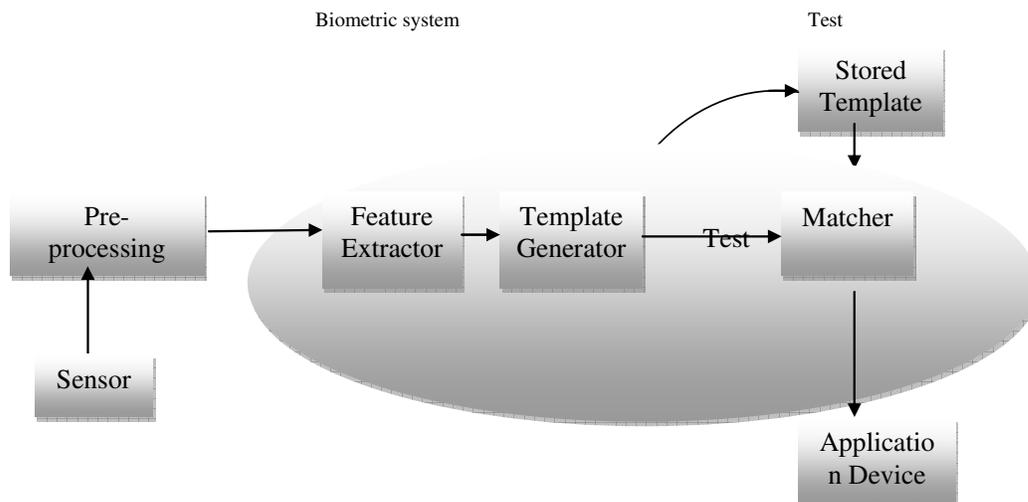


Figure 3: A block diagram of a biometric system (biometrica, 2012).

The diagram shows a simple block diagram of a biometric system. When such a system is networked together with telecommunications technology, biometric systems become 'telebiometric' systems. The main operations a system can perform are enrolment and test. During the enrolment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block features needed are extracted. This step is an important step as the correct features need to be extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identifiability.

If enrolment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).

3.4.1 Classification of biometrics

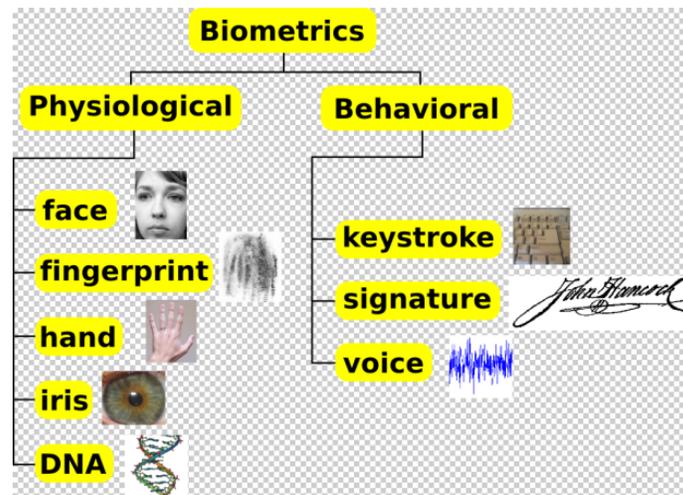


Figure 4: Classification of biometrics (biometrica, 2012).

3.4.1.1 Physical biometrics: these are related to the shape of the body. Examples include:

- Bertillonage – measuring body lengths (no longer in use)
- Finger print- analyzing fingertip patterns
- Facial recognition – measuring facial characteristics
- Hand geometry – measuring the shape of the hand
- Iris scan – analyzing features of colored ring of the eye
- Retinal scan – analyzing vein patterns
- DNA – analyzing genetic makeup

3.4.1.2 Behavioral biometrics: these are related to the behavior of a person. They are:

- Voice recognition – analyzing vocal behaviour
- Signature verification – analyzing signature dynamics
- Keystroke dynamics – measuring the time spacing of typed words.

4. IMPLEMENTATION, RESULTS & DISCUSSION

4.1. Performance evaluation of authentication mechanisms

Table 1: Advantages and Disadvantages of Authentication Mechanisms

Authentication mechanism	Advantages	Disadvantages
Pin and Password	<ul style="list-style-type: none"> ✓ Least expensive methods to use ✓ No need to install any hardware device ✓ There's no need to install any extra software for their usage. 	<ul style="list-style-type: none"> ✓ Weak and susceptible to numerous attacks ✓ Security depends on the user's ability to maintain the user ID and password secret ✓ Not fully reliable when used for making financial transactions remotely, such as fund transfers and bill payment through an internet banking channel.
(Pbworks, 2006)		
Smartcard	<ul style="list-style-type: none"> ✓ Users don't need to remember complex passwords ✓ It enhances the image of the organization by securing user credentials more effectively ✓ It can be used for login and transaction authentications. ✓ Individuals gain increased security and convenience when using smartcards ✓ It enhances privacy. 	<ul style="list-style-type: none"> ✓ Users need multiple tokens for multiple website and devices ✓ It involves additional costs, such as the cost of the token and any replacement feed. ✓ The plastic card in which the chip is embedded is fairly flexible, and the larger the chip, the higher the probability that the normal use could damage it ✓ It is not excessively trustworthy, since it can be stolen, lost or simply forgotten at home. ✓ Sometimes, they are combined with cryptography methods, which makes them more difficult to implement.
(Smartcardbasic, 2012).		
Biometrics	<ul style="list-style-type: none"> ✓ Difficult to compromise ✓ Can be used for accessing high-security systems and sites ✓ Information is unique for each individual and it can identify the individual in spite of variations in the time. ✓ Different options are available such as fingerprint, iris, or retina scanner authentication 	<ul style="list-style-type: none"> ✓ High deployment cost ✓ Involves additional hardware costs such as scanners, cameras etc ✓ May not be suitable for mass-consumer deployment ✓ It requires high cost of maintenance.
(Pbworks, 2006).		

Table 2 : Biometrics Comparison Chart (Pbworks, 2006).

Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

Table 3: Biometrics Comparison Chart (360biometrics, 2012).

Biometrics	Univer- sality	Unique- ness	Perma- nence	Collect- ability	Perfor- mance	Accept- ability	Circum- vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

Table 4: Biometrics Evaluations Chart(Debnath Bhattacharyya et al, 2009).

BIOMETRICS	EER	FAR	FRR	SUBJECTS	COMMENTS
Face	NA	1%	10%	37437	Varied light,indoor/outdoor
fingerprint	2%	2%	2%	25000	Rotation &exaggerated skin distortion
Hand geometry	1%	2%	2%	129	Improper placement
Iris	.1%	4%	.99%	1224	Indoor environment
keystrokes	1.8%	7%	.1%	15	During 6 months period
Voice	6%	2%	10%	30	Textdependent

4.1.2 Evaluation

There are various parameters with the help of which we can measure the performance of any biometric authentication techniques. These factors are described below.

Table 4.4 shows the evaluated vales of various evaluation techniques.

4.1.2.1 Factors of Evaluation

- **False Accept Rate (FAR) and False Match Rate (MAR):** The probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percentage of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.
- **False Reject Rate (FRR) or False Non-Match Rate (FNMR):** The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percentage of valid inputs being rejected.
- **Relative Operating Characteristic (ROC):** In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variable simplicity. A common variation is the Detection Error Trade-off (DET), which is an obtained using normal deviate scale on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- **Equal Error Rate (EER):** The rates at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly when quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.
- **Failure to Capture Rate (FTC):** Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.
- **Template Capacity:** It is defined as the maximum number of sets of data which can be input into the system.

5. CONCLUSION

We have critically looked at various authentication mechanisms available for access control. Authentication mechanisms such as authentication mechanisms such as PINs, Passwords, Smartcards and Biometrics have been analysed for their strengths and their weakness. Access control is very important in order to secure the resources from unauthorised users. We have also considered the difficulty in compromising these mechanisms as well as their implementation cost. For future works, we suggest more research in ethical hacking; this will expose more weaknesses of some of these authentication mechanisms

REFERENCES

1. Allan A. (2002), Biometric: Biometric how do they measure up? Gartner Research, 2002, p.1-5
2. Bhattacharyya D., Ranjan R., Alisherov F. and Choi M. (2009): "Biometric authentication review", computer science and engineering department, Lintage Institute of Technology, Kolkata, India.
3. Biometrics in the 21st century, findbiometrics.com. Retrieved July 13, 2006 from <http://www.findbiometrics.com>
4. Caelli W. (2001): "Information security handbook", Stockton press, new york, p.20-22.
5. Cappelli R., Maio D., Maltoni D., Wayman J. and Jain A.K. (2006): "Performance Evaluation of fingerprint verification systems", IEEE Trans, volume 28, issue 1, pp.3-10.
6. Dimitriadis C.K. (2007): "Analysing the Security of Internet Banking Authentication Mechanisms", retrieved from <http://www.smartcardalliance.org>
7. Guthery S. and Jurgensen T.M. (2001): "Smartcard developer's kit", Macmillan technical publishing. ISBN 1-57870-027-2.
8. Jain A.K., Flynn P. and Ross A. (2007): "Handbook of Biometrics". Retrieved from
9. <http://www.biometrica.com>
10. Lander S. (2010): "Winding your way through DNA ", Centre for genome research, University of California, San Francisco, USA.
11. Matyas V. and Riha Z. (2001): "Biometric Authentication Systems", Technical report. Retrieved from <http://www.ecom-monitor.com/papers/biometrics>.
12. Morris R. and Thompson K. (1995): "Password security", Bill laboratories. Retrieved from <http://www.en.wikipedia.org/wiki/password>
13. Rankl W. and Effing W. (2001): "Smartcard handbook", John Wiley and sons. ISBN 0-471-96720-3.
14. Ritter R.M (2007): "The oxford style manual", Oxford University Press pp.12-13.
15. Robinson S. (2011): "Using Biometry for Security and Identification". Retrieved Aug, 2011 from <http://www.brighthub.com/>
16. Sahoo S.K., Choubisa T. and Prasanna M. (2012): "Multimodal Biometric person authentication", A review. IETE technology review. p54-60.
17. Shepherd-Barron J. (2010): "working of automatic teller machine (ATM)" retrieved from
18. <http://www.circuit.com>
19. Smartcard alliance identity council (2007): "identity and smartcard technology", retrieved from <http://www.smartcardalliance.org>
20. Winer P. (2003): "Security and authentication technologies", big chef partners, Inc.