

Unit V

TOPICS

Biometric Authentication Applications

access control like a lock or an airport check-in area

immigration and naturalization

welfare distribution

military application

banking, e.g., check cashing, credit card, ATM

topics

- *computer login; intruder detection; smart card*

multi-media Communication; WWW and an electronic purse

sensor fusion; decision fusion

categorization: e.g., age and gender

industrial automation

gesture interpretation

topics

efficient enrollment

audio-visual tracking

stock market

on-line shopping

compact embedded systems

other commercialized services

Most common application

- Logical Access Control;
- Physical Access Control;
- Time and Attendance;
- Law Enforcement;
- Surveillance.

*Access Control like a
lock? or an Airport
check in area ✈*

Introduction:

- ***Biometrics** are physical or behavioral human characteristics to that can be used to digitally identify a person to grant access to systems, devices or data. Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence.*
- *While the earliest accounts of biometrics can be dated as far back as 500BC in Babylonian empire, the first record of a biometric identification system was in 1800s, Paris, France.*
- *Alphonse Bertillon developed a method of specific body measurements for the classification and comparison of criminals.*

Access Control:

- In access control, there are three fundamental methods for verifying authorized access:
 1. *Something you know*: such as a password, a PIN, or a code
 1. *Something you have*: such as a key, an access card (or badge) or a mobile device
 1. *Something you are*: a physical trait, such as a fingerprint, also known as **biometrics**.

Something you are - biometrics

- In comparison to other forms of access authorization, the use of biometrics in access control is a more recent phenomenon.
- Biometrics describes a physical feature unique to a person which can therefore be used to identify that person.
- Types of biometric authentication include fingerprints, irises, facial recognition through contours and features, hand geometries, vein patterns, voice patterns and DNA information.
- Biometrics appear to be an ideal solution for authorization verification as the physical traits used are unique to each person. However, biometrics are not exempt from risk.

The reality:

- A recent survey of security integrator companies by IPVM, an impartial third party in the security industry, found that the demand for biometric solutions in security is actually still quite low. The most popular type of biometrics opted for from the above was fingerprint recognition at 49%, but 44% of integrators chose to use no biometrics at all.
- The possible reason for this apparent reluctance to implement biometrics in access control is because many professionals think that the technology is largely under-developed and needs further technological progress. Moreover, some companies hold back from adopting biometrics for fear of conflicting with local privacy restrictions or of infringing on the personal privacy of employees or personnel.

Biometrics at Airport:

- There is an End – to – End process going on at airport Nowadays.

- Before you reach the airport :
 1. Before you even reach the airport, biometrics is improving your overall experience. To start, many states around the world now require biometric identification as part of the VISA application process. In the UK, for instance, you can share your digital identity – in the form of fingerprints or a facial scan – with the authorities to expedite your application and the pre-screening process.
 2. Moreover, airports are beginning to trial new forms of mobile check-in to provide a seamless and secure way of preparing passengers for their flight before travel.
 3. London's Heathrow Airport, for instance, has partnered with Yoti to allow travelers to use their smartphones as a means of verifying their identity. Passengers use their faces to check-in and store the tickets on their phones, which are then used to authenticate the passenger's identity during each touchpoint within the airport.

At the airport (Check In):-

- When you arrive at the airport, biometric technology is helping to automate the verification process, meaning that you move swiftly and safely through border control. It's all about airlines delivering the best possible passenger experience for you.
- One way in which they have been doing this is through the integration of Automated Border Control technology or [eGates](#), as they are more commonly known eGates compare your passport to a photo capture of your face to verify you are who you say you are. It's an easier, less intrusive and fast experience that can help combat fraud and it's much more reliable than the traditional fingerprint scan.
- Moreover, biometrics is helping to remove the hassle of multiple checks while in the airport. Whether you're purchasing goods in duty free or about to board the flight, biometrics will eliminate the need for you to present your boarding pass or passport to verify your identity.
- Instead, you will be a biometric token – based on facial recognition software – which allows you to move about the airport freely and securely.

At Check In the security system are as below:



In-flight and on the other side:

- Biometrics does not stop improving the passenger experience when you're in-flight either. Through the use of [digital identities](#) (in which your biometric data is stored) your personal information can be shared with border control to expedite the immigration process. Just think – no more long lines after you step off a flight, meaning you can relax on your holiday as soon as possible.
- Furthermore, as you've used biometrics to drop your luggage off before your flight, you can now use that same biometric 'token' to collect your bags hassle-free.
- All-in-all, it means getting to where you want to go, faster, efficiently and most importantly, in a secure fashion.
- This is how Biometrics is developed all over the world.

IMMIGRATION AND NATURALIZATION

- Security is the main concern in immigration and naturalization service.
- Biometric authentication helps to run background checks and to ensure that the person does not have criminal records which can be a threat to national security.

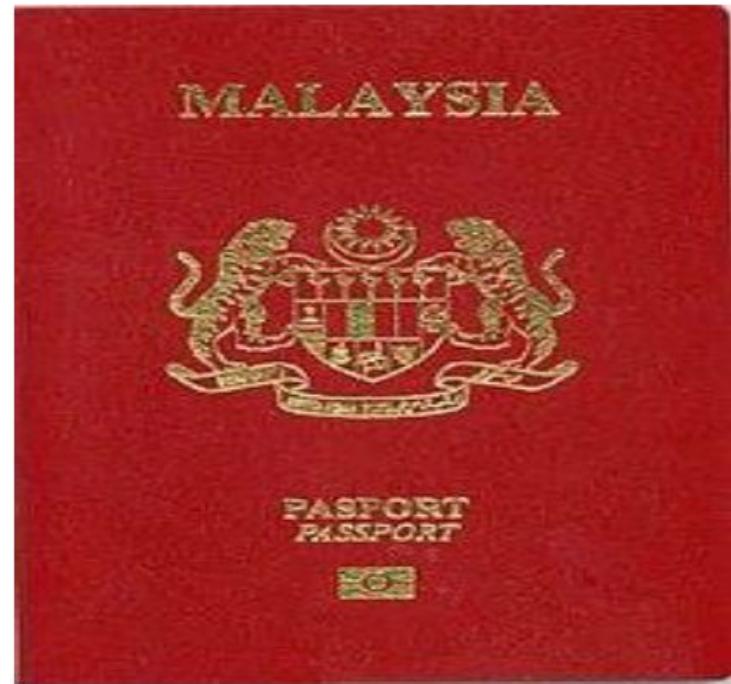
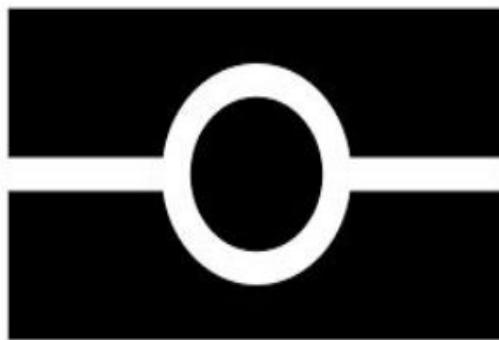
FIRST IMPLEMENTATION

- Malaysia was the first country to issue Biometric passports in 1998. A biometric passport is a traditional passport that has an embedded electronic microprocessor chip which contains biometric information that can be used to authenticate the identity of the passport holder.
- The biometric data that was included on the malaysian passport is a digital photograph of the bearer's face and images of the two thumbprints.
- Malaysian Immigration checkpoints were the only ones with the technology to read and authenticate the data from the RFID chip using fingerprint scanner and facial recognition technology

- HAND SCAN TECHNOLOGY is used for employee access control and passengers facing implementations.
- Different sensors are used to authenticate travellers information by capturing their fingerprints.
- Due to advancement in Artificial Intelligence and specific technologies like deep learning and Convolutional Neutral Netwoks, face recognition is improved dramatically in last few years. This is an important recognition because of cost-effective and accurate in identity recognition.

PASSPORT

BIOMETRIC PASSPORT



Gesture recognition

- Gesture recognition has been defined as the mathematical interpretation of a human motion by a computing device.
- Due to COVID-19 this technology s is introduced in airports to people can communicate with public devices without to touchthem.

Abu Dhabi Airport deploys Gesture Recognition to elevators to prevent COVID-19 spread



@GlobalInnovation

Body Temperature Screening System

- Due to current scenario of COVID-19, PopID has introduced body temperature screening system.
- Employees have to enroll a photo for biometric facial recognition through PopID website and can present themselves before the fixed biometric device for instant temperature checking and identification with or without the mask.
- Temperature measurement results are reported within seconds and employees use a thumbs-up or thumbs down gesture to complete the health survey questions appearing on the screen.

Welfare Distribution

Biometric identification systems can also help governments to more equitably distribute welfare benefits to the poor. Biometrics are unique and a faster and more efficient identification mechanism to ensure the right people are receiving the right benefits. Many countries who are affected by corruption can take full advantage of this technology to more equitably distribute public services such as welfare.

But Before that, lets categorise what exactly comes under distribution of welfare:

1. Ration Distribution
2. Education Scholarship Fund Distribution
3. Disaster Relief Distribution

Possibilities of Biometrics:

Biometric National ID

Biometric Voter Registration (BVR)

ePassport



Beyond Touchscreens : The perils of biometric social welfare in lockdown (

Case Study)

Gradually over the last years, India has introduced biometric identification of users in most of its social welfare schemes. One of the main such schemes is the Public Distribution System (PDS), the nation's largest food security programme, which provides rationed subsidised commodities to the nation's poor through a network of ration shops. Biometric access to the PDS is largely operated through Aadhaar, the world's largest digital identification scheme which provides enrollees with a 12-digit number and capture of biometric credentials (ten fingerprint and iris scans) for recognition.

As a consequence of the COVID-19 crisis, biometric authentication in ration shops has been suspended in several Indian states. A commonly given reason for this is the risk of disease transmission associated to users' fingerprint contact with the machine



Welfare Distribution

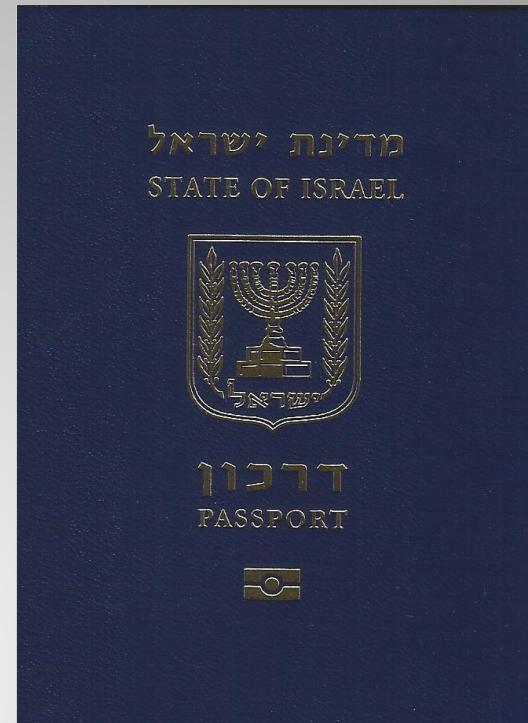
Implementation

Australia : Visitors intending to visit Australia and returning Australian residents with an ePassport may have to submit to biometric authentication as part of the [Smartgate](#) system, linking individuals to their visas and passports. Biometric data are collected from some visa applicants by Immigration particularly in cases of Refugee or Humanitarian Visas.

Brazil : By the end of 2005, the Brazilian government started the development of its new passport. The new documents started to be released by the beginning of 2007, in Brasília. The new passport included several security features, like laser perforation, UV hidden symbols, security layer over variable data etc. Brazilian citizens will have their signature, photo, and ten rolled-fingerprints collected during passport requests.



Israel : In 2009, the Knesset (Israeli Parliament) passed the Biometric Database Law, sanctioning the issue of biometric ID cards and passports to all Israeli citizens and the establishment of a mandatory database for storing their bodily information (fingerprints and face templates). In 2013, Israel launched a two-year preliminary pilot study to evaluate and assess the project's feasibility and necessity, in which participation was voluntary.



USA : NEXUS is a joint Canada-United States program operated by the Canada Border Services Agency and U.S. Customs and Border Protection. It is designed to expedite travel cross the US-Canada border and makes use of biometric authentication technology, specifically iris recognition biometric technology. It permits pre-approved members of the program to use self-serve kiosks at airports, reserved lanes at land crossings, or by phoning border officials when entering by water

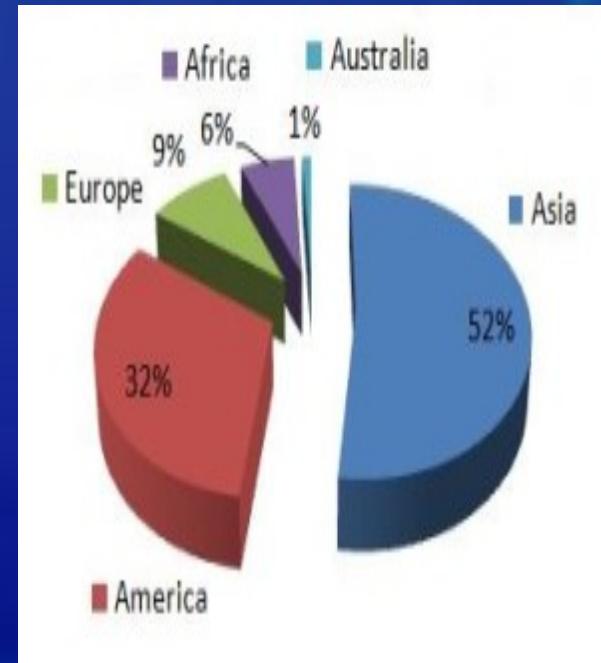


Impact of Biometrics in Banking

- The rapid digitization of banking services combined with the continued need to adopt stricter customer and employee identification protocols to prevent identity theft and fraud has set the table for biometric identification technology to become an integral and strategic part of financial service security platforms. Acting as a strong authentication tool to help secure ATM, brick and mortar, and online transactions, biometrics in banking also helps to increase customer trust and improve brand reputation. The necessity for a stronger authentication solution became inevitable in banking services because of the growing pace of sophisticated transactional technology adoption along with the unfortunate rise in fraud and security breaches due to reliance on traditional security systems such as passwords

Biometric Technology in the Banking Sector

- Biometrics are automated methods of recognizing customers through their biological characteristics and traits such as fingerprints, finger vein patterns, iris, and voice recognition. Biometric characteristics are unique for every individual and difficult to forge, which is why biometric verification and authentication is commonplace in immigration control, law enforcement, and forensic studies. Many banks worldwide are already using biometrics with their banking systems to authenticate employees and customers and among all banks utilizing biometrics, 52 percent are located in Asia. Japan has more than [an estimated 15 million customers using biometric authentication for banking transactions.](#) Banks in Mexico, South America, Africa, and the Middle East are also moving towards the use of biometric identification technology because of its popularity with consumers, and ability to offer more security than traditional personal identification numbers (PINs) and passwords.
- Proportion of Banking Using Biometric in Different Continents



Different Usage of Biometrics in Banking

Biometric technology is slowly replacing traditional passwords and token-based electronic access, signature-based branch service access, and PIN-based access in mobile banking and at ATMs. Here are ways that banks can use biometric technology to improve banking services and better protect customer assets:

- **Biometrics in Branch Banking**— When customers visit branches they can be authenticated at the counter through fingerprint and finger vein biometric scanners that match the customer's existing biometric template within the bank database, and after successful authentication, the customer will be allowed to move forward with their banking transactions.
- **Biometrics in Banking ATMs**- Using biometrics in banking ATMs is popular in developed countries and the adoption rate is growing significantly. There are two approaches for customer authentication in ATMs — a customer using only biometrics and a bank card or a PIN along with biometric authentication. Therefore, facial recognition, fingerprints, finger vein patterns and iris recognition are the most suitable in ATMs as these biological traits can be easily authenticated in this environment. Furthermore, these types of biometric modalities also have other advantages such as flexibility, compactness, and accuracy.
- **Biometrics for Internet Banking**- Many computers, laptops, and even smart phones already have webcams, microphones, and fingerprint scanners, offering flexibility for banks to easily adopt biometric authentication in online banking services with fingerprint, finger vein, facial, and voice recognition. When customers attempt to access their accounts online, they will be required to provide their biometric information to verify their identity.

- **Biometrics in Mobile Banking**- Mobile banking is growing rapidly worldwide, and according to [Juniper Research](#), 400 million people performed a mobile banking transaction in 2013. Despite this large number, many bank customers still have a lack of trust over the security of mobile banking platforms and concerns over security. Banking transactions or customer services could be performed through a voice or speech recognition system where customers need to verify their identity using the microphone in their phones. Voice biometrics has many advantages for both the financial institution and the consumer. It streamlines the authentication process by removing the need for additional equipment a human operator all together – lower operational costs significantly; complex passwords and PINs are no longer required; the authentication process needn't be duplicated and, more significantly, the use of voice biometrics in the call centre and other channels can prevent information obtained from data breaches from being used. From the consumer perspective, it all also allows all actions and transactions to be managed from any device, anywhere
- **Single Sign on Solution for More Effective Password Management** - Banks and financial institutions are suffering from network security and data breaches worldwide. According to a recent [ACI Worldwide Survey](#), 44% of customer financial accounts have been compromised and 15% of breaches cause fraud. In a 2013 [Ponemon Institute Survey](#), it was reported that an average cost of these types of incidents is \$9.4 million. Banks can easily adopt [biometric single sign on](#) (SSO) solutions into their network for password management, identity

Benefits of Using Biometrics in Banking

- **Protecting Banking Information** – Biometric technology provides the strongest method of authentication that protects banking information from being compromised by unauthorized personnel.
- **Fast and Accurate Branch Banking** – Biometric technology provides fast and accurate identification for the banking industry. Customers can be quickly authenticated in mere seconds through a fast biometric scan.
- **Protection Against Insider Fraud** – Biometric identification of employees performing transactions on the back end is a crucial step to ensuring identity protection and reducing fraud. Biometrics in banking will help financial institutions to prevent insider fraud by establishing secure employee authentication, accountability and concrete audit trail of each transaction.
- **Secure Online Banking** – Over the past years the banking sector has been suffering from massive online service cyber attacks. In most of these cases customers lose their money from the negative effects of identity theft. Biometrics in banking helps the bank to protect customer identities when using online banking services.

- **ATMs with Biometrics** – Biometrics in banking for ATMs authentication brings outstanding benefits to both customers and banks. This system now gives customers flexibility to make transactions without bringing bank cards. Banks can avoid the costs and liabilities of customer problems due to lost or stolen bank cards.
- **Audit Trails** – Banks can easily track and monitor employee and customer activity in the system to create concrete audit trails with biometric technology solutions.
- **Fast, Secure and Accurate Customer Care Service** – The banking sector is always in need of tighter security solutions to provide improved and more secure customer care service over the phone and internet. A biometric voice recognition system for example provides a secure and flexible solution to verify any customers executing transactions outside of a brick and mortar environment.

Due to the role of customer trust and loyalty in the success of banks, and thus in the economic development of countries, banks should provide convenient and more secured banking services to customers. Biometric technology, integrated with an existing traditional security system, will empower banks to deploy the highest level of authentication security possible.

military

- In Army, access control is necessary for weapons systems. These systems increasingly consist of physical, logical and informational components.
- Unauthorized use of any single system can have adverse consequences .
- In peacetime, access control issues are also important because of improving the effectiveness and efficiency of the Army operations.
- Since Army operates a vast set of human resource services(healthcare, retiree, dependent benefits troop support services etc), access control is necessary to verify claims and to reduce fraud.
- Biometrics is a possible solution for army's Access control problems. The push for Biometrics is driven by its both technical possibilities and political interests.

Military Challenges

- It is found that the demands placed on its biometric systems by the military were far tougher than the commercial world and came up with innovative solutions to the challenges presented.
- For example, capturing iris prints outdoors in the Middle East on a hot, sunny day was difficult as the individuals tended to squint.
- Whereas historically iris capture is carried out at a distance of about 20 inches so your irises are in the open, we re-engineered the system so you put your eyes up to what looks like a set of binoculars. That encloses your eyes from the light and we get a really good capture of the irises.

Merits of Biometrics in Defence

The benefits of implementing biometrics in defence and intelligence are manifold, but let us have a look at some unavoidable and considerable merits:

- Accurate identification of the military personnel to recognize any unidentified encroachment.
- Can help in improving national security.
- Easily tracks any unauthorized access within the premises.
- Protects confidential places, information, etc.
- Identifying an individual (Army personnel and civilians) at border areas.
- Securely stores the biometric data obtained from combatant commands and military services.

SENSOR FUSION AND DECISION FUSION

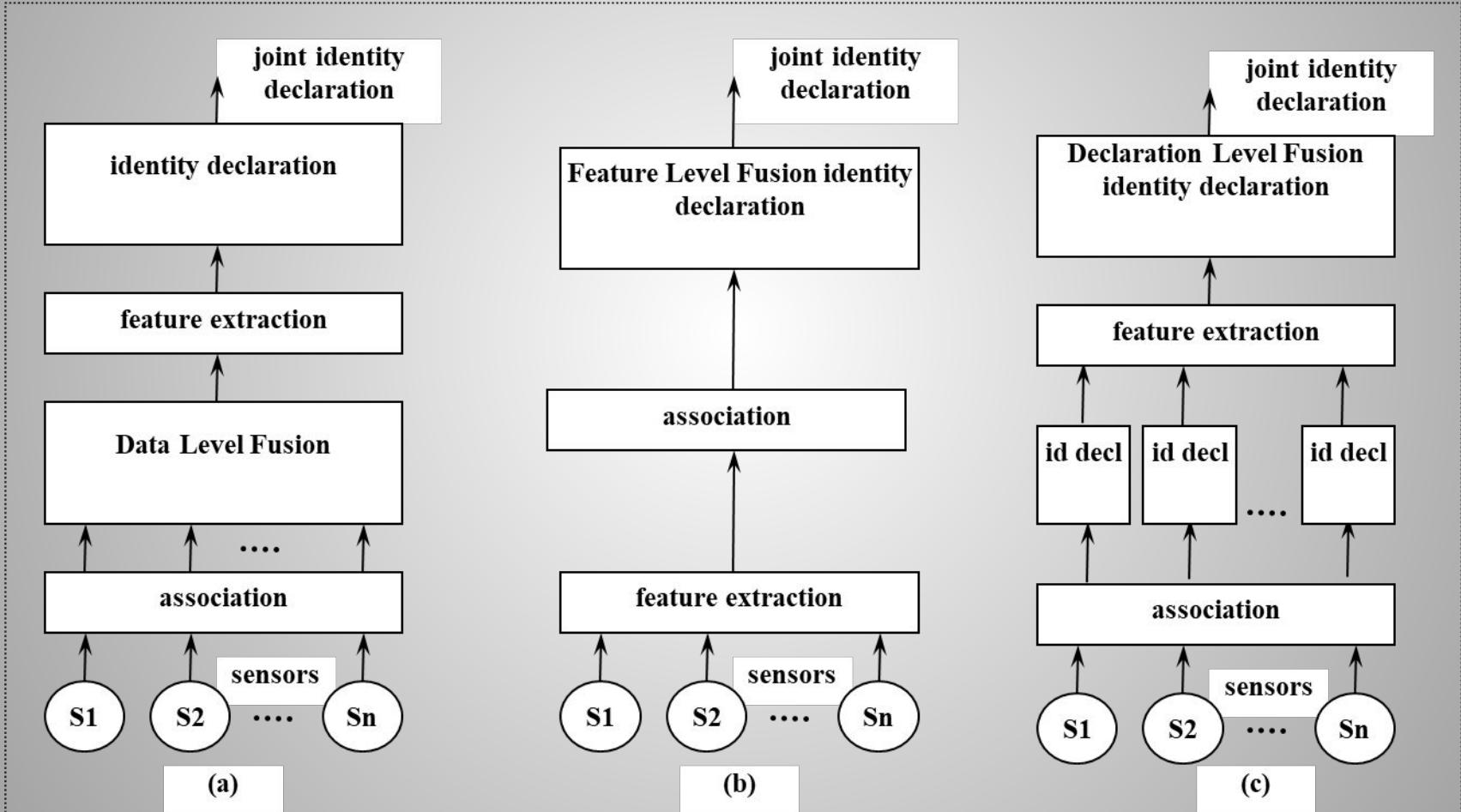
SENSOR FUSION ?

- **Sensor fusion** is combining of sensory data or data derived from disparate sources such that the resulting information has less uncertainty than would be possible when these sources were used individually. (less uncertainty means more accurate or complete)
- Combining 2 or more data sources in a way that generates a better understanding of the system.
- Sensor fusion is also known as (*multi-sensor*) data fusion and is a subset of information fusion.
- The process of combining data or information to estimate or predict entity states.

Examples of sensors ↗

- Cameras
- Accelerometers
- Sonars
- Electromagnetic sensors
- Radars
- Etc.....

SENSOR FUSION ARCHITECTURES



Sensor fusion as a technique covers various known algorithms?

- CENTRAL LIMIT THEOREM
- KALMAN FILTER
- BAYESIAN NETWORKS
- DEMPSTER – SHAFER
- CONVOLUTION NEURAL NETWORKS

APPLICATIONS OF SENSOR FUSION

- GPS/INS ☐ Global Positioning System and inertial navigation system data is fused using various different methods, e.g. the extended Kalman filter. This is useful for determining the altitude of an aircraft using low-cost sensors.
- TRAFFIC STATE ☐ Traffic in a road can be categorised as low traffic, traffic jam and medium flow by combining the data of road side acoustics, road images and sensor data.
- Building various autonomous systems.

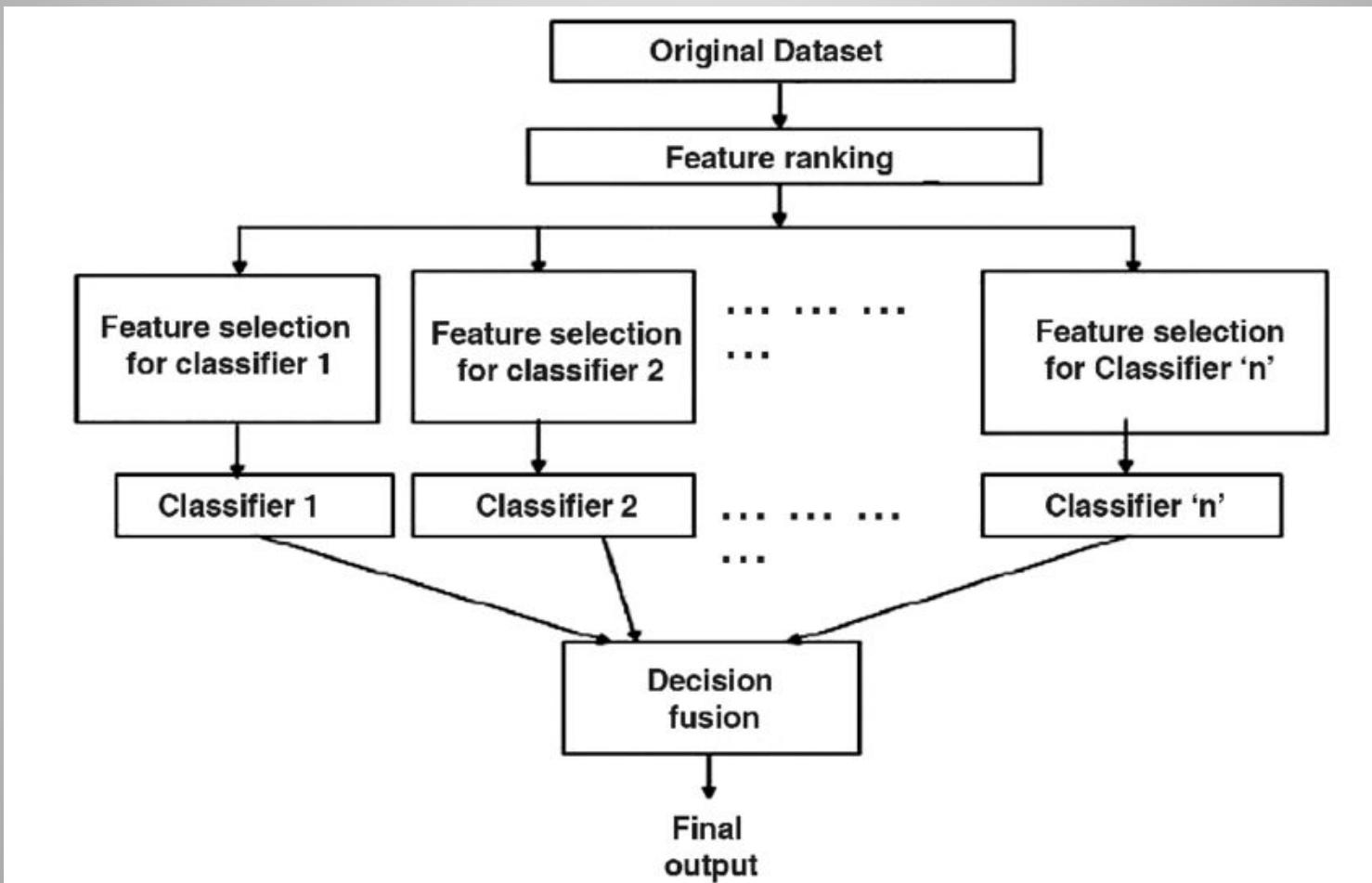
DECISION FUSION

- Decision fusion is one form of data fusion that combines the decisions of multiple classifiers into a common decision about the activity that occurred.
- Decision fusion is defined as the concept of combining information from different data sources, after each source has been classified individually.

VARIOUS CLASSIFICATION ALGORITHMS USED

- Logistic Regression.**
- Naïve Bayes.**
- Stochastic Gradient Descent.**
- K-Nearest Neighbours.**
- Decision Tree.**
- Random Forest.**
- Support Vector Machine.(SVM)**

Basic representation



APPLICATIONS ?

- Construction of mansions (or simply architecture).
- Autonomous driving .
- Image forensics.
- Etc....

Computer Login

Computer login process can be performed using biometric authentication.

Biometric authentication refers to security processes that verify a user's identity through unique biological traits.

Biological traits used for computer login

- Retinas
- Irises
- Voices
- Facial Characteristic
- Fingerprints

intrusion detection system(Ids) and Intruder detection

- Intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.
- In information security, intruder detection is the process of detecting intruders behind attacks as unique persons. This technique tries to identify the person behind an attack by analysing their computational or biometric behaviour.

- Some of the parameters used to identify an intruder are
 1. Keystroke dynamics
 2. Patterns using an interactive command interpreter
 3. Patterns on the network usage

SMART CARD

- A smart card or chip card is a physical electronic authorization device, used to control access to a resource.
- It is typically a plastic credit card-sized card with an embedded integrated circuit(IC).
- Smart cards can provide personal identification, authentication, data storage, and application processing.
- Applications include identification, financial, mobile phones(SIM), public transit, computer security, schools and healthcare.

HISTORY

- The basis of the smart card is the silicon integrated circuit (IC) chip.
- Invented by Robert Noyce in 1959 and made possible by Mohamed M. Atalla's silicon surface passivation process and Jean Hoerni's planar process.
- Smart Card idea was first introduced by Helmut grottrup and Jurgen Dethloff in 1960s.

TYPES OF SMART CARDS

1. Contact Smart Cards
2. Contactless Smart Cards
3. Hybrids
4. USB

APPLICATIONS

- Financial
- SIM
- Public Transit
- Video Games
- Computer Security
- Schools
- Healthcare

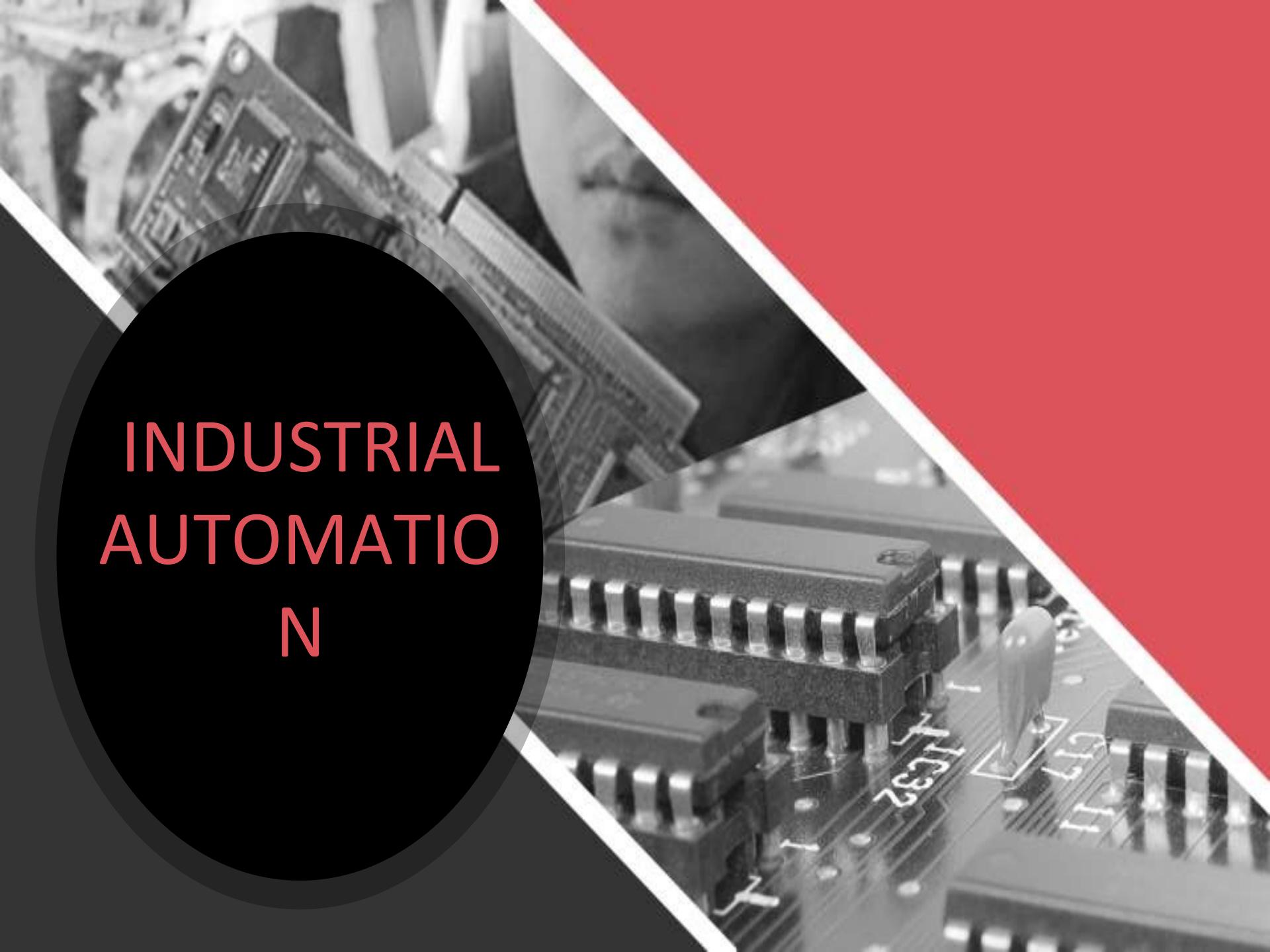
Benefits

- Volume of information and applications can be programmed for use on a card.
- Multi-factor and proximity authentication increase the security of the smart card exponentially.
- Governments and regional authorities save money.
- Individuals have better security and more convenience with smart cards.

Disadvantages

- The plastic or paper card in which the chip is embedded is fairly flexible.
- The production, use and disposal of PVC plastic is known to be more harmful to the environment than other plastics.
- If the account holder's computer hosts malware, the smart card security model may be broken.
- Smart Cards have been the targets of security attacks.
- Lack of standards for functionality and security.

INDUSTRIAL AUTOMATIO N



WHAT IS AUTOMATION?

Automation is basically the delegation of human control function to technical equipment for



Increasing Productivity



Increasing Quality



Reducing Cost



Increasing Safety in working conditions

TYPES OF AUTOMATION



Buildin



Lig
ht



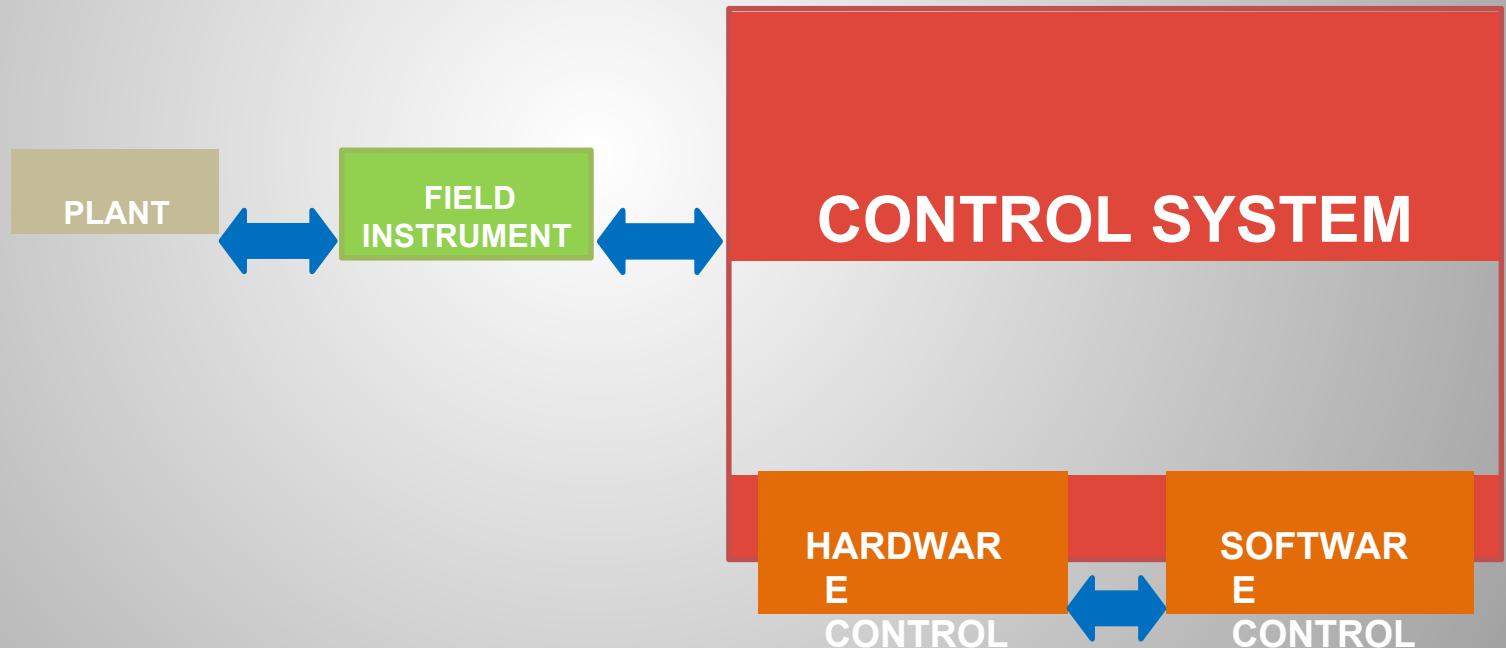
Scien
tic



Industri

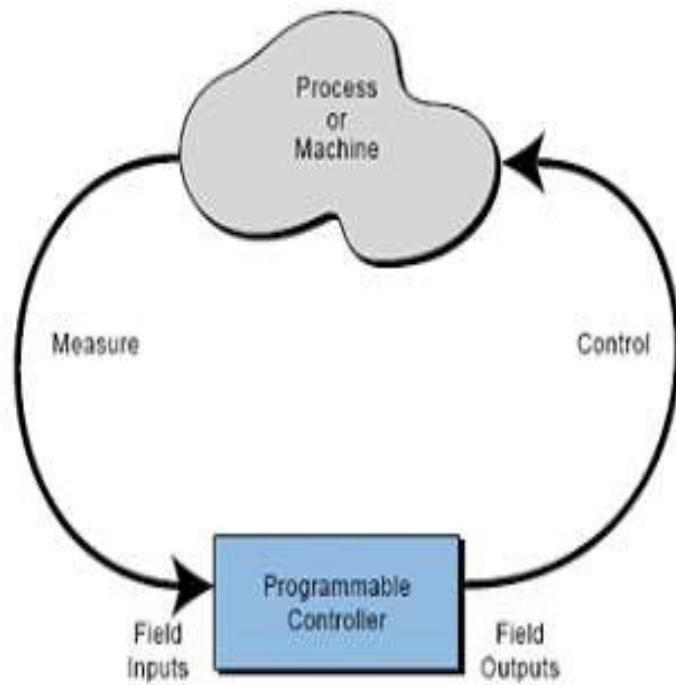
INDUSTRIAL AUTOMATION

- use of control systems, such as computers or robots, and information technologies
- for handling different processes and machineries



Programmable Logic Controller

- industrial computer that monitors inputs and makes decisions
- based on its program and controls outputs to automate a process
- specialized to handle incoming events in real-time
- PLC is a **digital computer** designed for **multiple inputs and output** arrangements
- it has input lines where sensors are connected to notify upon events
- and output lines to signal any reaction to the incoming events
- uses a programmable memory to store the instructions

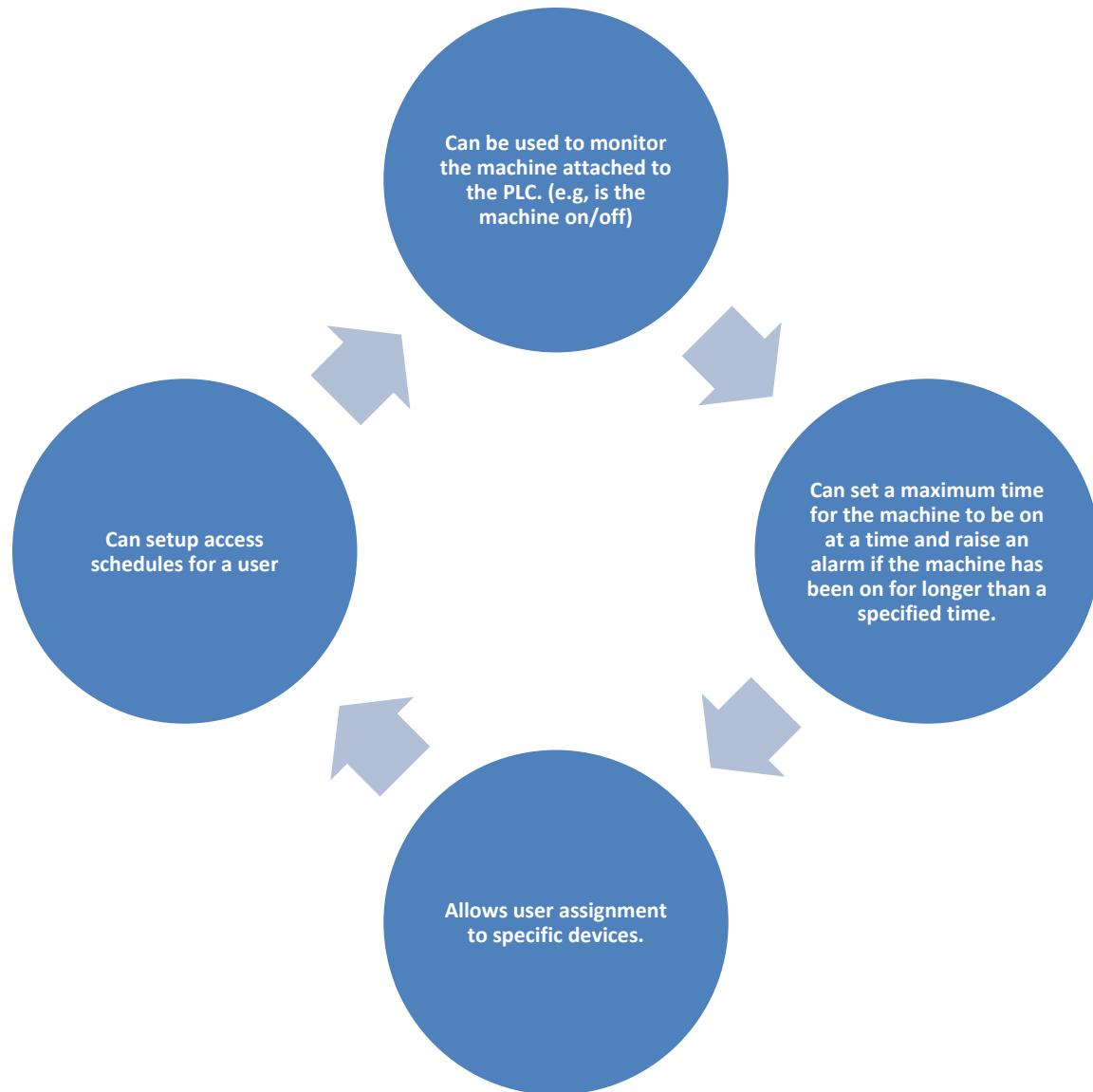


Biometrics in Programmable Logic Controller

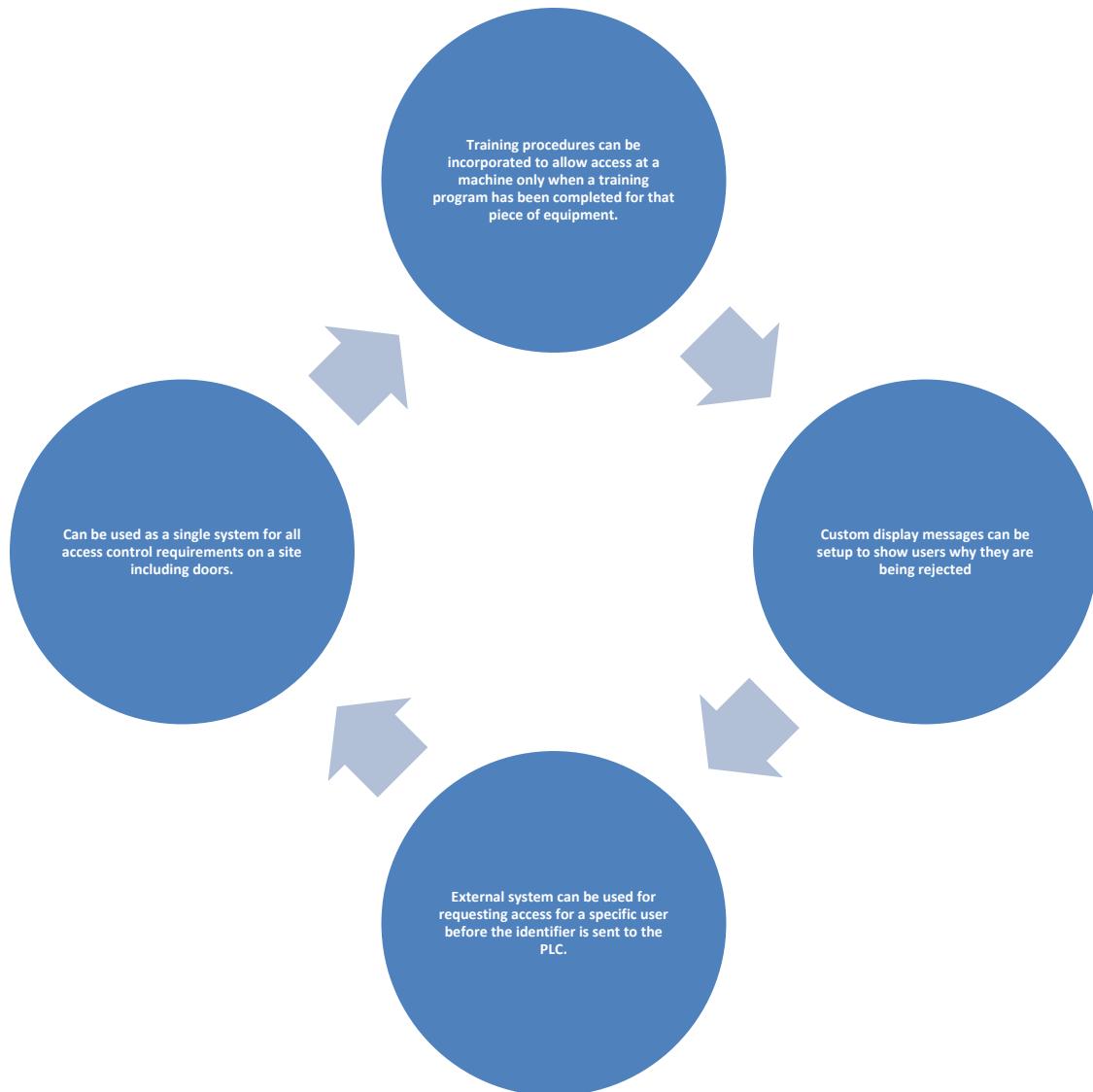
We use fingerprint authentication to identify the person and then we pass ASCII data to your PLC in a variety of ways so that the PLC can then supply the programming you provided to it. We work on a variety of connections like RS422, RS485 and ethernet. Give us a call and we can take you through what it will take for your site to be up and running using Biometric PLC Access control just like a Global Top 3 Auto Manufacturer is doing today.



BiometricPLCAccess is useful for PLC integration in the following ways:



BiometricPLCAccess is useful for PLC integration in the following ways:



Biometric Authentication System x +

researchdesignlab.com/biometric-authentication-system-for-plc-and-scada.html

welcome! My Account | My Wishlist | My Cart | Checkout | Log In

support | faq | knowledge base

CUSTOMER SUPPORT
Monday-Saturday 10am-6pm
+91 824 2988407

All Search entire store here... 0 items in cart. Checkout >

Interfacing Board Modules Wireless Development Board Sensors DIY Kits Components Robot Kits

[Home](#) / Biometric Authentication System for PLC and SCADA



Biometric Authentication System for PLC and SCADA

Email to a Friend

★★★★★ 5 Review(s) | [Add Your Review](#)

[Sign up for price alert](#)

[Like 27](#) [Share](#)

RDL Biometric Add on Block product is designed to seamlessly integrate with the shop floor machinery. The flexible and customizable design allows you to control various operations like switching machine job operation, down time escalation and product loss escalation.

The product is tested with all major PLC vendors and supports multiple interface options.

ORDER CODE: RDL810

Availability: In stock

₹13,500.00 Qty: 1 [Add to Cart](#)

[Add to Wishlist](#) [Add to Compare](#)

Product Description Tags (0) Reviews (5)

Leave a Message

Desktop 06:22 PM 09-11-2020 ENG

Categorization on the basis of Age & Gender



- Information on the gender of a person plays a vital role in crime investigation, authentication and statistical report on the visitors.
- Fingerprint ridge count and fingertip size are used as the parameters for automatic gender classification.
- The optimal score assignment (OSA) method is proposed to classify gender

Body parts which we can use to categorize people on the basis of Gender:

- 1.Nose
- 2.Eyebrows
- 3. Eyelashes
- 4. Hairstyle



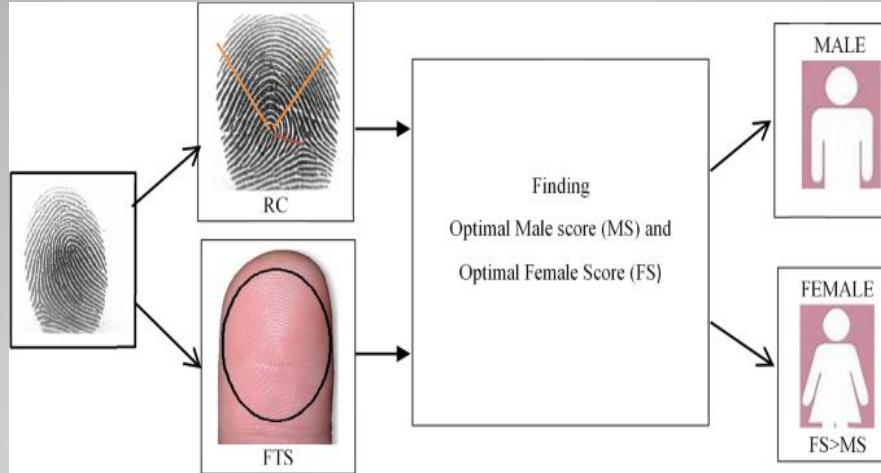
- Generally, the male nose is comparatively larger. Similarly, the bridge and ridge of the male nose are also more significant
- Eyebrows also help in gender recognition. Female eyebrows are longer, thinner, and curly at the ends. On the other hand, male eyebrows are mismanaged and thicker



- It can be observed from face images that females have larger eyelashes, which are curly. Our CRFs based segmentation model classifies these eyelashes with hair
- Hairstyle has very complex geometry, which varies from person to person. segmentation model extracts the hairline efficiently. We encode this information as a feature descriptor and use it in our gender classification algorithm.

fingerprints

Ridge patterns exhibit many properties that reflect the biology of individuals. Ridge parameters such as fingerprint ridge count, ridge density, ridge thickness to valley thickness ratio, ridge width and fingerprint pattern types are used for gender determination.



The gender of the person is judged using the fingerprint of that concern person based mostly on the count of the ridges of the fingerprint. The average ridge count is slightly higher in males than in females, with high standard deviation among subjects of each gender



USING BIOMETRICS TO FIND AGE OF THE PERSON

The forensic investigators always search for fingerprint evidence which is seen as one of the best types of physical evidence linking a suspect to the crime. Discrete Wavelet Transform (DWT), the Singular Value Decomposition (SVD) and Principal Component Analysis (PCA) has been used to estimate a person's age using his/her fingerprint. Mostly K nearest neighbour (KNN) is used as a robust classifier

GESTURE INTERPRETATION

Overview

What is gesture interpretation?

Types of gesture interpretation

1. Offline gestures
2. Online gestures

Algorithms

Application

Advantages



What is gesture interpretation

- - 1 Gestures can originate from any bodily motion or state but commonly originate from the face or hand.
 - 2 Users can use simple gestures to control or interact with devices without physically touching them.
 - 3 Gesture recognition can be seen as a way for computers to begin to understand human body language.



Types of gesture interpretation

1. Offline Gestures
 2. Online Gestures
- 

Offline Gestures

Gestures that are processed after the user interpretation with the object.

Eg - Swiping the screen with palm to take a screenshot

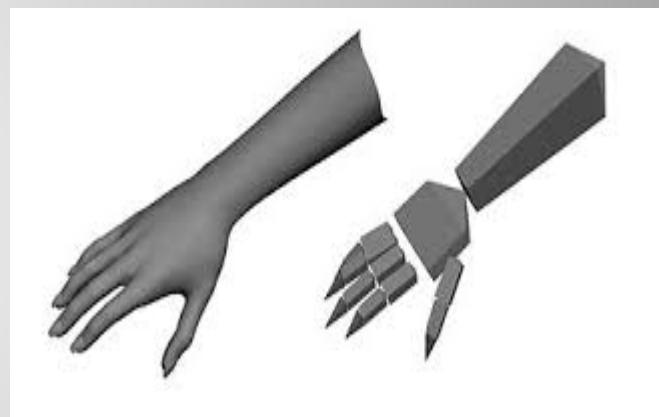
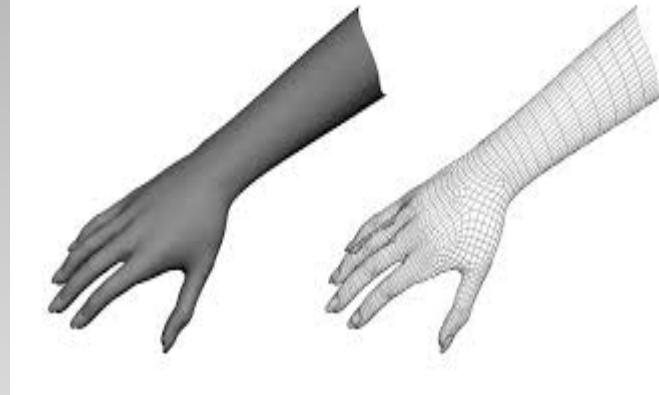
Online Gestures

Direct manipulation gestures. They are used to scale or rotate a object mostly.

Eg - Pinching fingers inwards or outwards to zoom in or zoom out.

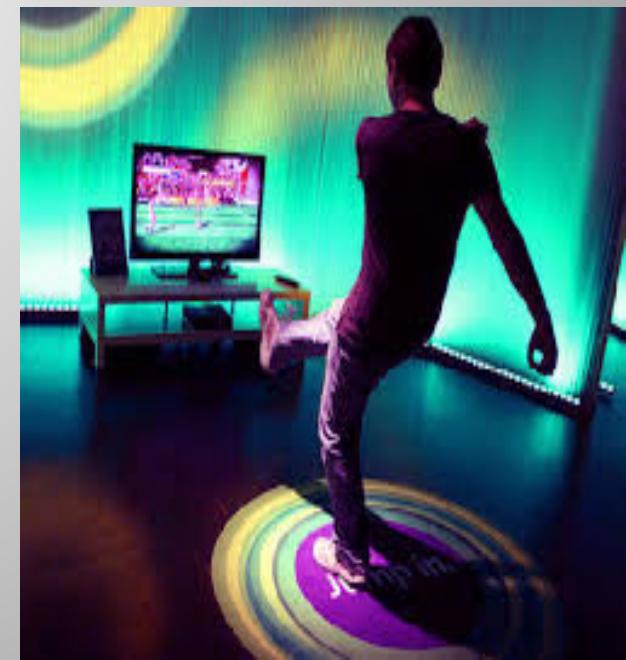
Algorithms

- 1 3D model based
- 2 Skeletal based
- 3 Appearance based models



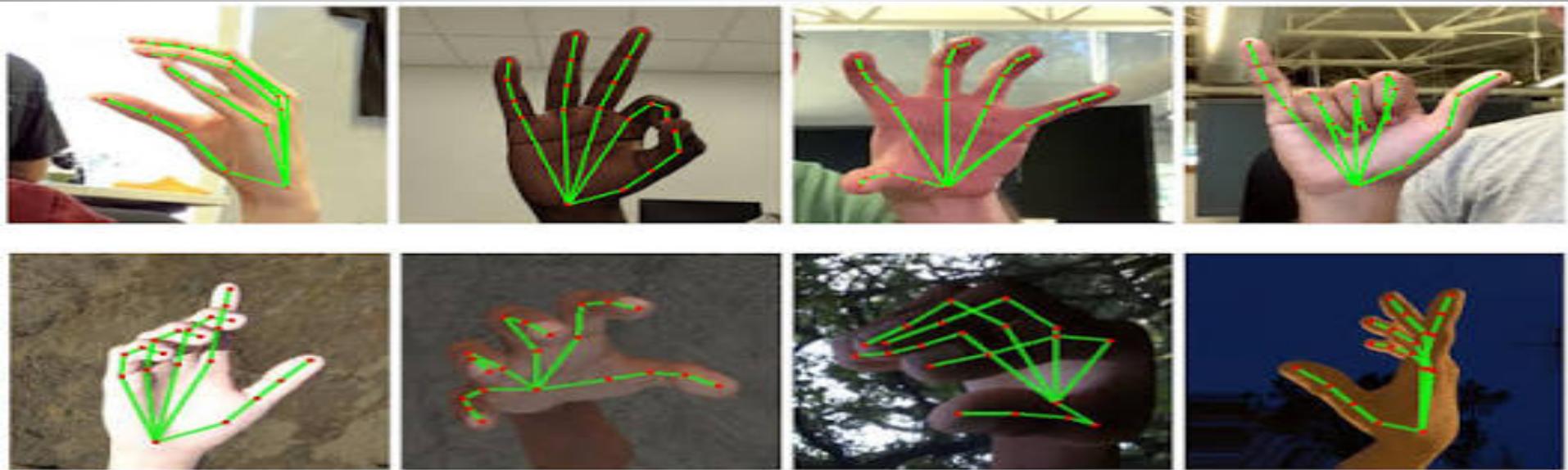
Applications

- 1 Gaming sector
- 2 Smartphone devices
- 3 Home automation
- 4 Automated sign language translation
- 5 Defence



Advantages

- 1 Operating without touching.
- 2 A more natural form of communication with device.



BIOMETRICS

AUDIO-VISUAL TRACKING

INTRODUCTION

- Visual information conveys correlated and complimentary information to the audio information.
- Its integration into a recognition system can potentially increase the system's performance.

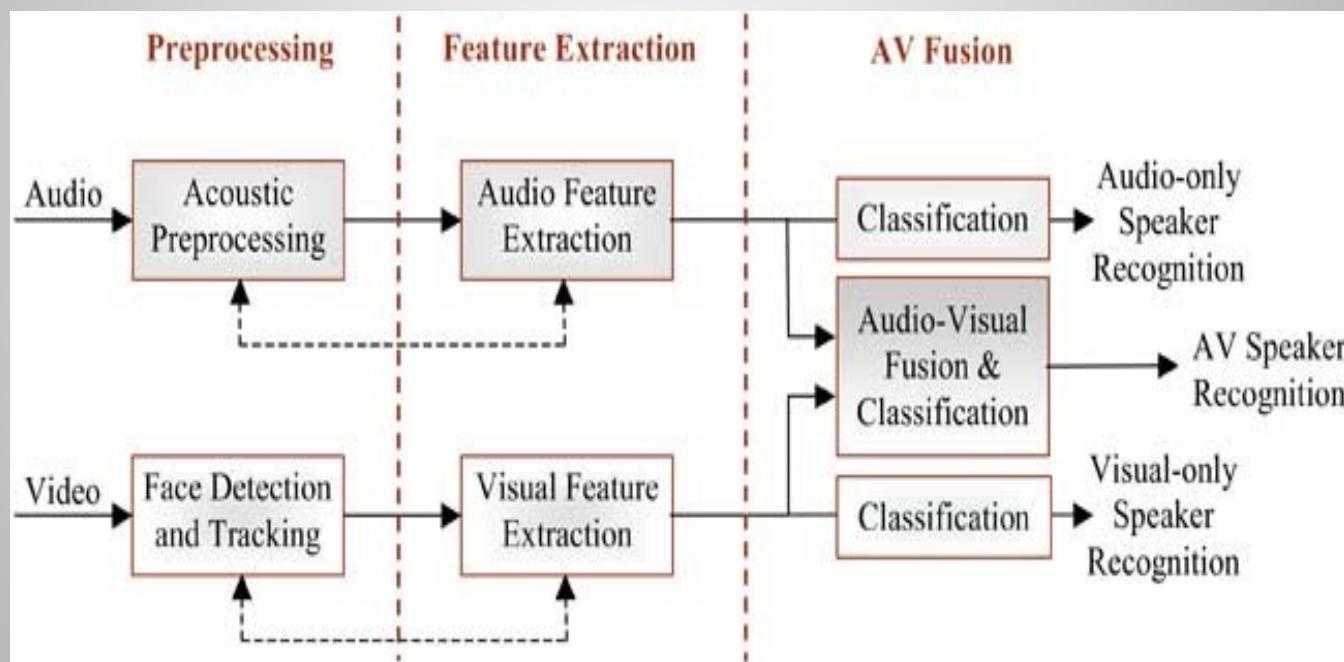
- AV person recognition is one of the most promising user-friendly low-cost person recognition technologies that is rather resilient to spoofing.

Importance of AV Biometrics

- Face visibility benefits speech perception.
- There exists a strong correlation among face motion, vocal tract shape, and speech acoustics.
- Plays an important part in the development of human– computer interaction (HCI) systems.

AV BIOMETRICS SYSTEM DESCRIPTION

Block diagram of AV biometrics system



- The AV person recognition system consists of three main blocks:
 1. pre-processing
 2. feature extraction and
 3. AV fusion.

- Pre-processing and feature extraction are performed in parallel for the two modalities.
- Pre-processing includes: signal enhancement, tracking environmental and channel noise, feature estimation, and smoothing.

ANALYSIS OF VISUAL FEATURES UTILIZED FOR AV BIOMETRICS

- Visual features are usually extracted from 2-D or 3-D images.
- Facial visual features can be classified into global or local.
- Visual features can also be either static or dynamic.

- The various sets of visual facial features are generally grouped into three categories:
 - 1) appearance-based features
 - 2) shape-based features
 - 3) features that are a combination of both appearance and shape features.

SPEAKER RECOGNITION PROCESS

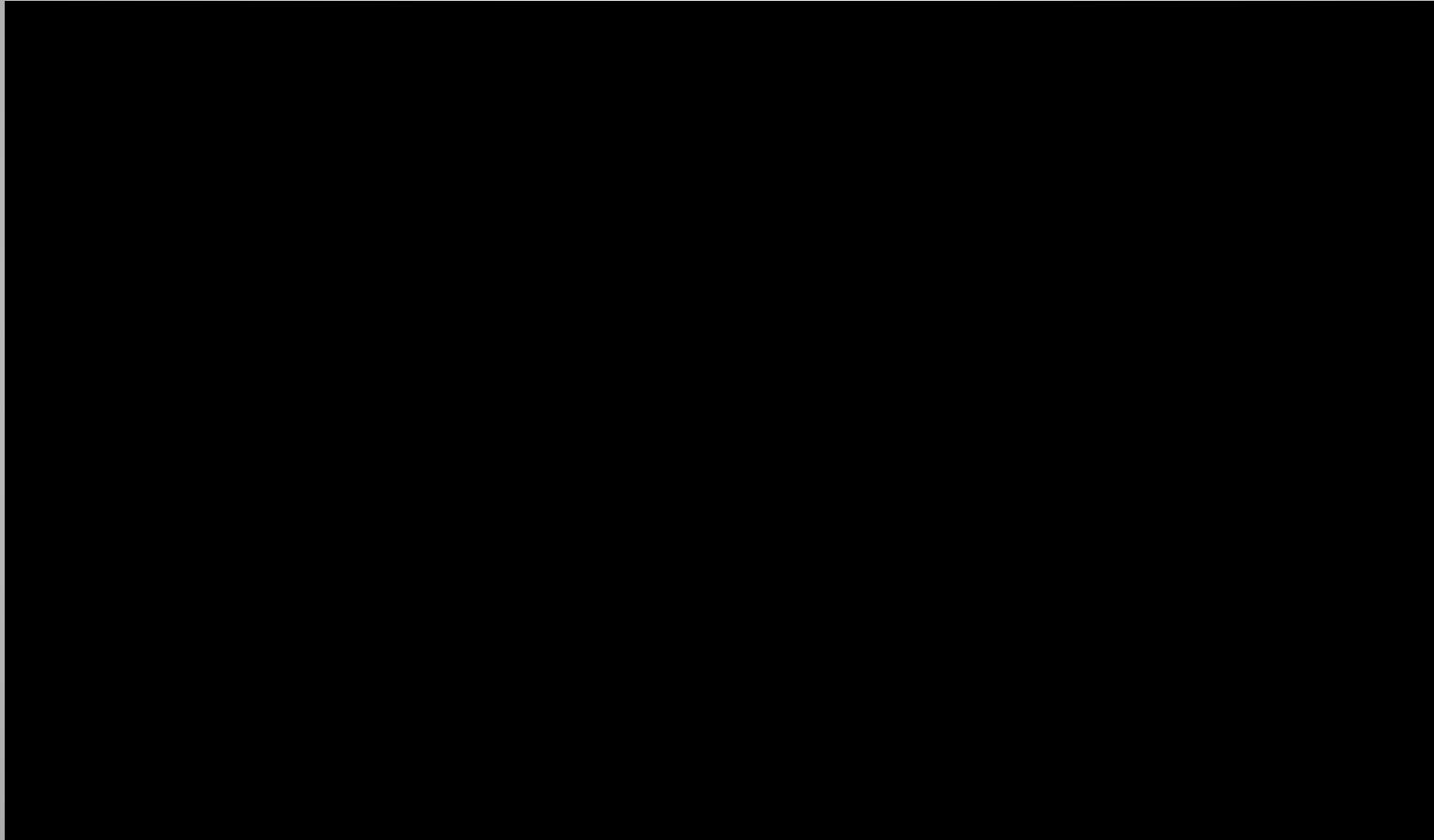
- Speaker recognition systems can be classified into text-dependent and text-independent.
- Text-dependent systems can be further divided into fixed-phrase or prompted-phrase systems.

- Fixed-phrase systems are trained on the phrase that is also used for testing.
- Prompted-phrase systems ask the claimant to utter a word.
- In the text-independent systems, the speech used for testing is unconstrained.

AV FUSION METHODS

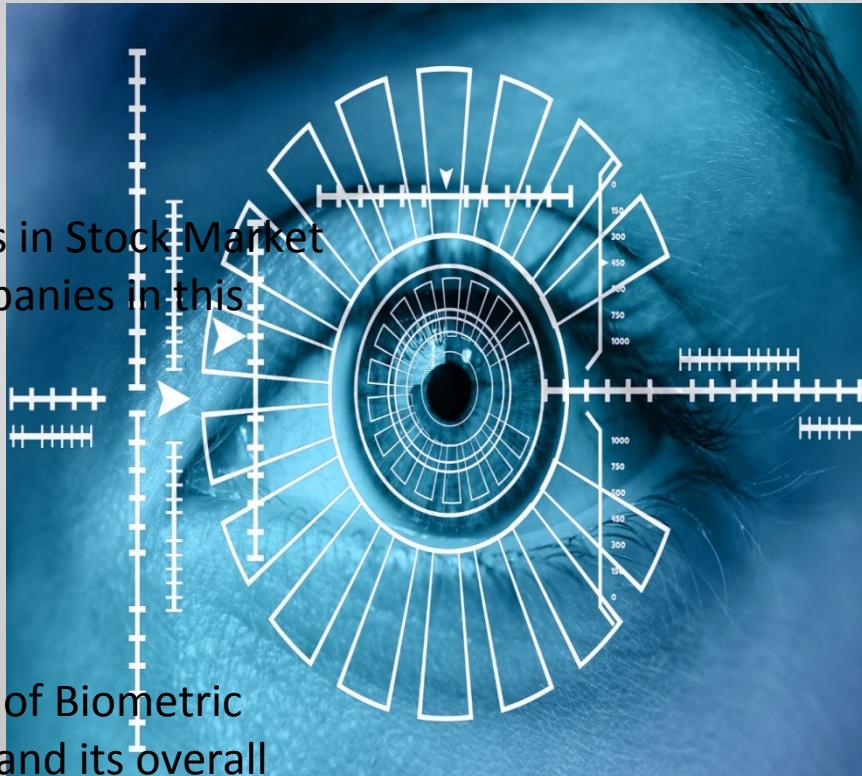
- Fusion approaches are usually classified into three categories:
 1. Pre-mapping fusion
 2. Midst-mapping fusion
 3. Post-mapping fusion

AV FUSION METHODS



Effects of Biometric Systems on Stock Market

- Brief History
- Role of Biometrics in Stock Market
- Top Leading Companies in this sector
 - SYNAPTICS
 - GENTEX
 - NVIDIA
 - ALIBABA
 - FaceX
- Future Projection of Biometric Systems Industry and its overall valuation



Brief History

- It was first implemented in 1960s where the facial features were taken and feature points were extracted from it manually. As due to lack of technology in that times, the procedure took too much time to recognize a particular feature or even extract it.
- In 1991, facial recognition technology was developed, which made in-real time recognition possible. Though, there were a lot of faults, it had skyrocketed the implementation of facial recognition
- While in 2007, Toshiba released their first fingerprint implemented phone called g500, which wasn't a huge success but it led to Apple releasing 5s in 2013, having better implementation and very fast matching system, It made the smartphone industry jump into the biometric system, booming the Biometrics into the Stock Market.



Role of Biometrics in Stock Market

- So, Biometrics does play a role in Stock Market sector as its wide series of implementations on different security devices and hardware, led to huge production of capacitive scanners and cameras, which are capable of real-time facial recognition and data capturing. Some of the leading companies are Synaptics, Gentex, Nvidia and Alibaba.



- Synaptics

Known earlier for their touchpads for laptop computers, SYNA has advanced to areas such as fingerprint biometrics technology for smartphones.

Synaptics drives the industry's most dynamic markets with innovative products designed for both established and emerging markets.

As we dive further into the digital era, I believe SYNA stock will deliver long-term gains for current stakeholders.



• Gentex

- One of the top artificial intelligence stocks, Gentex offers several automotive safety features, including blind-zone indicators and forward-looking sensors. Anything that can help distracted drivers is a plus in my book.
- Most of the Gentex products are based on biometric systems and its use cases. It's also a leader in the automobile safety industry which makes it a valueable and high-end achieving stock in the future.



• Nvidia

- One of the most famous companies, with its exclusive Ray Tracing Technology in its Graphics Card, making the overall process faster, It also pioneered smart-surveillance technologies.
- This technology allows law enforcement to quickly track down suspects and persons of interest. It's AI-powered surveillance program constantly scans faces 24/7.
- While most people recognize NVDA as a gaming-centric semiconductor firm, the company also is one of the most compelling facial recognition stocks.



- Alibaba

The latest leap of Alibaba is **facial recognition** technology that allows a customer to pay by literally flashing a smile at Kentucky Fried Chicken (KFC).

As facial recognition stocks improve in sentiment and visibility, I think Alibaba has a competitive edge.

First, China has 1.4 billion people with almost everyone providing the data to fulfill the advancement of technologies with facial recognition and even better automation via gestures.

Alibaba is the leading company, topping the biometric stocks to its edge.



- FaceX

FaceX's technology employs state-of-the-art tracking technology to detect people even under low illumination and varied poses.

That is not all, it also detects people at far distances, even when the face is pixelated very badly to the human eye. Further, it recognises faces with an accuracy rate of 94%.

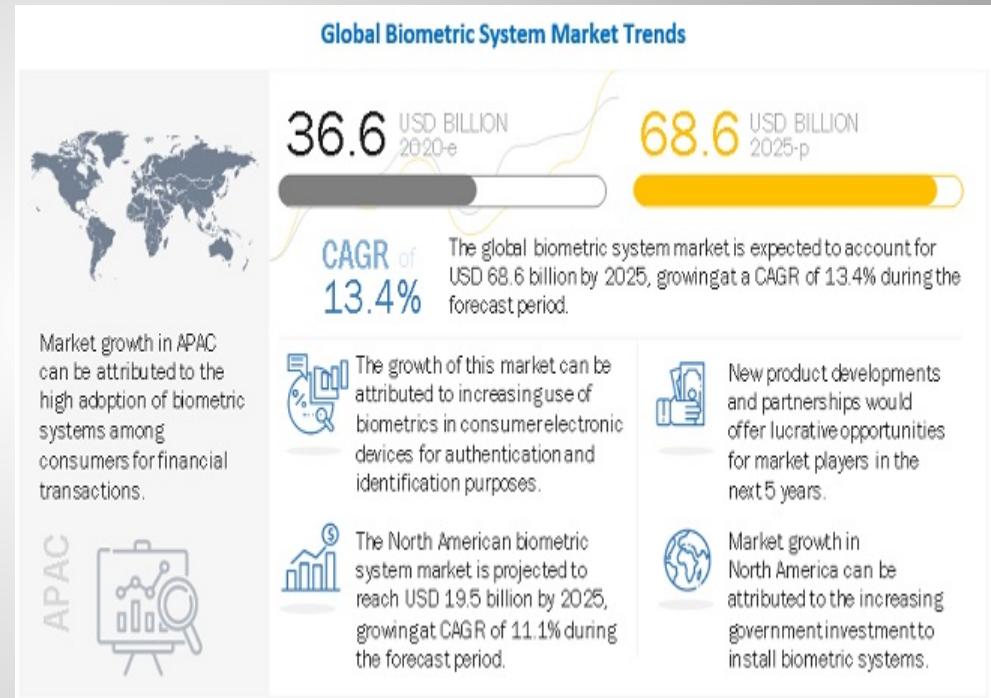
It is an Indian Startup and in its Investing rounds. Till It hits the IPO Sector, It could be a major breakthrough like the Indian ML Startup, AINDIA.



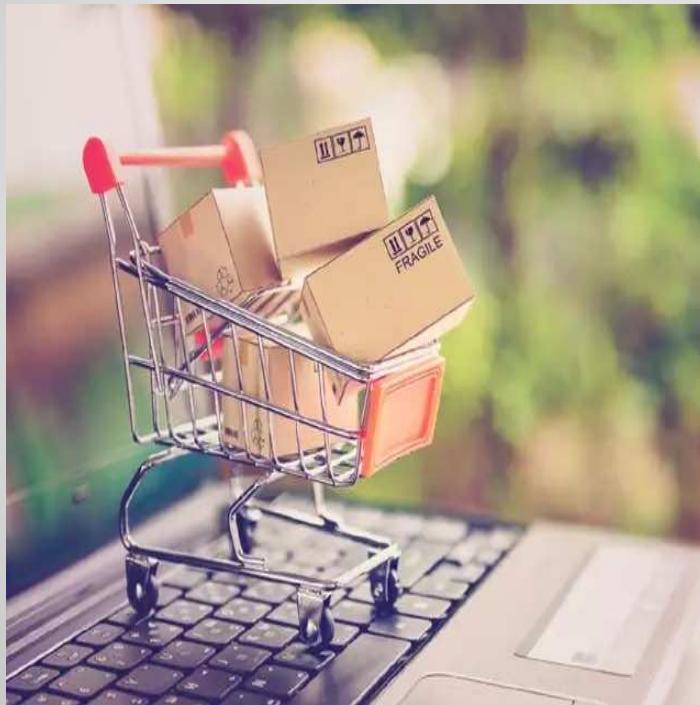
Future Projection of Biometric Systems Industry and its overall valuation

So, the overall Biometric System market is valued at 36.6 Billion Dollars, but it will increase dramatically due to exposure of hands-free technology in Covid, which gave a huge boost to the Biometric Industry.

This type of boost will give a different space in the Tech Sector of the Stock Market and Its evaluation will be way more than the predicted analysis, according to the situation and high-end innovations coming in the market.



ONLINE shopping



Introduction

- Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the internet.
- It's a B2C process. ie Business to consumer ecommerce.
- Online customers must have access to the internet and a valid method of payment in order to complete a transaction.
- Online stores are usually available 24 hours a day.

Modules



- Admin can login the system
 - Admin can create categories
 - Admin can upload products
 - Admin can upload product features
- the users can login the system
 - The buyers can search for a particular product
 - The buyers can order a product

Is it secure ?

- Traditional security methods like remembering a username, password, and a secret question are now outdated because hackers can easily break them and get access to user accounts. In such cases, the systems do not recognize the true identity of a user and allow anyone to sign in to an account whoever has a password.



How biometrics is applicable to online shopping ?



Eliminating frauds

- Biometrics assists customers in retaining their identity rather than remembering passwords, codes, or secret questions.
- Different technologies of biometrics distinguish users with a unique identity which is hard to attain for others.
- Fingerprints are among the oldest traits of biometrics used for recognition because of the lining pattern that varies person to person.
- Voice recognition belongs to behavioral biometrics of an individual and considered an effective technique in safeguarding user accounts from fake access
- Facial biometrics is a widely acceptable method for granting secure access to online shops. It works by scanning the face of every individual, capturing it in an image or video, and transforming it into a code to be compared with the already available code in the database.

Benefits of biometrics in Online shopping

- An end to stolen or forgotten passwords
- Automatic positive identification of users
- Enhanced security measures
- Forging is made difficult for intruders
- Non-transferrable accounts

MULTI – MEDIA COMMUNICATION

Multimedia communication deals with the transfer, protocols, services, and mechanisms of discrete media data (such as text and graphics) and continuous media data (like audio and video) in/over digital networks.

Such a communication requires all involved components to be capable of handling a

well-defined quality of service (QoS). The most important QoS parameters are used to request:

- 1) the required capacities of the involved resources,
- 2) compliance to end-to-end delay and jitter as timing restrictions, and
- 3) restriction of the loss characteristics.

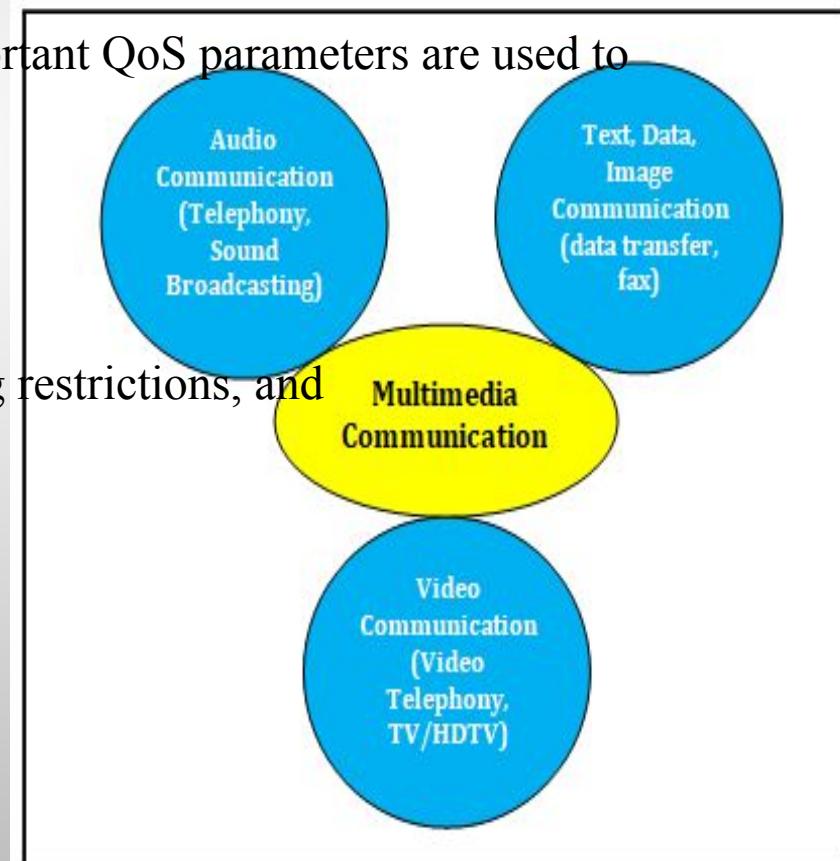
Characteristics:

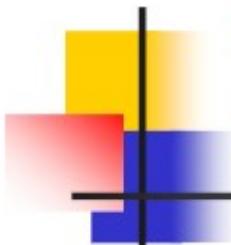
- *Highly delay-sensitive:*

Packets that incur a sender-to-receiver delay of more than a few hundred milliseconds (for Internet Telephony) to a few seconds (for streaming of stored media) are essentially useless.

- *Loss Tolerant:*

Occasional losses only cause





Security Standards for Multimedia Communication

- IPsec
 - Security services for the Internet Protocol
 - It is mandatory for IPv6 and optional for IPv4.
 - Encapsulating Security Payload (ESP)
 - Authentication Header (AH)
- H.235
 - H.235 standard describes security services for H.323.
 - Baseline Security Profile
 - Message authentication/integrity for the signaling path.
 - Voice encryption profile
 - Signature Security Profile
 - Authentication, integrity, and non-repudiation for the signaling messages by using digital signatures.
- SRTP
 - The Secure RTP (SRTP) provides confidentiality and authentication for RTP and RTCP.
 - The encryption of SRTP or SRTCP packets is optional whereas the authentication for RTCP is mandatory but optional for RTP.

ADVANTAGES

- It is very user-friendly.
- It is multi sensorial.
- It is integrated and interactive.
- It is flexible.
- It can be used for a wide variety of audiences, ranging from one person to a whole group.

DISADVANTAGES

- Information overload.
- It takes time to compile.
- It can be expensive.
- Large files make it unpractical and slow.
- Over the internet there are a few factors to keep in mind, for example bandwidth and the user's abilities.

WORLD WIDE WEB [WWW]



Advantages of the Internet;

1. Faster Communication

✓ The foremost target of Internet has always been speedy communication and it has excelled way beyond the expectations. Newer innovations are only going to make it faster and more reliable..

2. Information Resources

✓ Information is probably the biggest advantage that Internet offers. Internet is a virtual treasure trove of information. Any kind of information on any topic under the sun is available on the Internet.

3. Entertainment

Entertainment is another popular reason why many people prefer to surf the Internet. Downloading games or just surfing the celebrity websites are some of the uses people have discovered.

4. Social Networking

Social networking has become so popular amongst youth that it might one day replace physical networking. Apart from finding long-lost friends, you can also look for job, business opportunities on forums, communities etc.

5. Online Services

The Internet has made life very convenient. With numerous online services you can now perform all your transactions online. You can book tickets for a movie, transfer funds, pay utility bills, taxes etc., right from your home.

6. e-commerce

The concept of e-commerce is used for any type of commercial maneuvering or business deals that involves the transfer of information across the globe via the Internet. It has become a phenomenon associated with any kind of shopping, business deal etc.



Disadvantages of the Internet;

1. Theft of Personal Information

If you use the Internet for online banking, social networking or other services, you may risk a theft to your personal information such as name, address, credit card number etc.

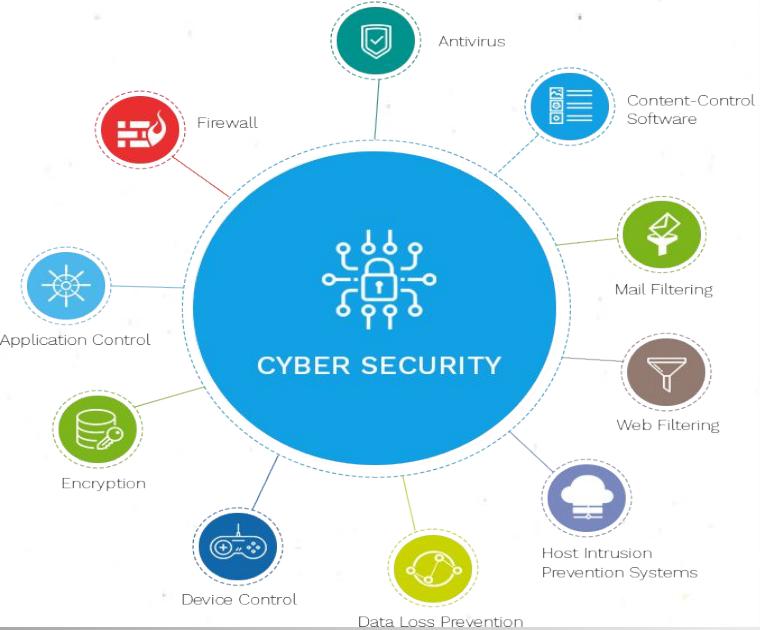
2. Spamming

Spamming refers to sending unwanted e-mails in bulk, which provide no purpose and needlessly obstruct the entire system. Such illegal activities can be very frustrating for you as it makes your Internet slower and less reliable.

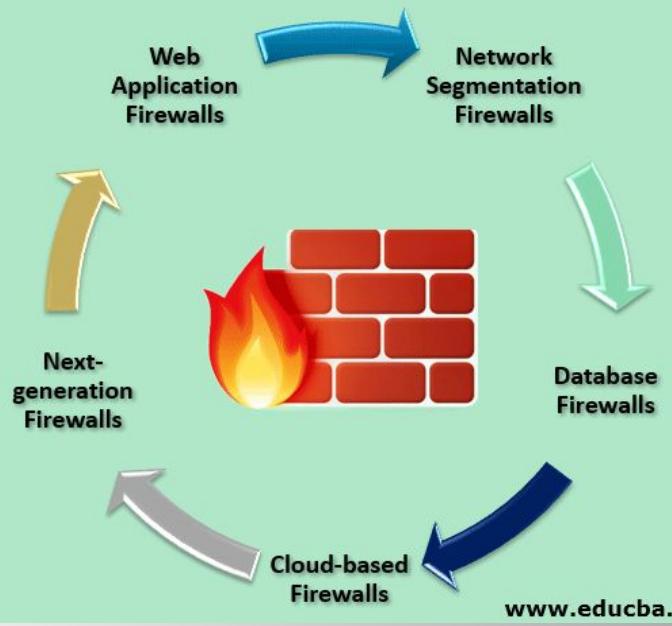
3. Virus Threat

Internet users are often plagued by virus attacks on their systems. Virus programs are inconspicuous and may get activated if you click a seemingly harmless link. Computers connected to the Internet are very prone to targeted virus attacks and may end up crashing.





Types of Firewalls



Black Hats

Individuals with extraordinary computing skills, Restoring to malicious or destructive activities and also known as Crackers



Grey Hats

Individuals who work both offensively and defensively at various times



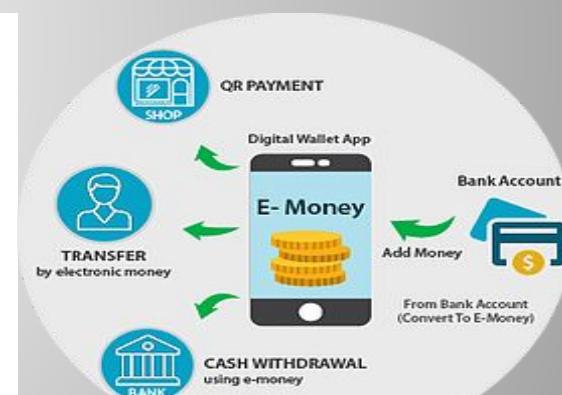
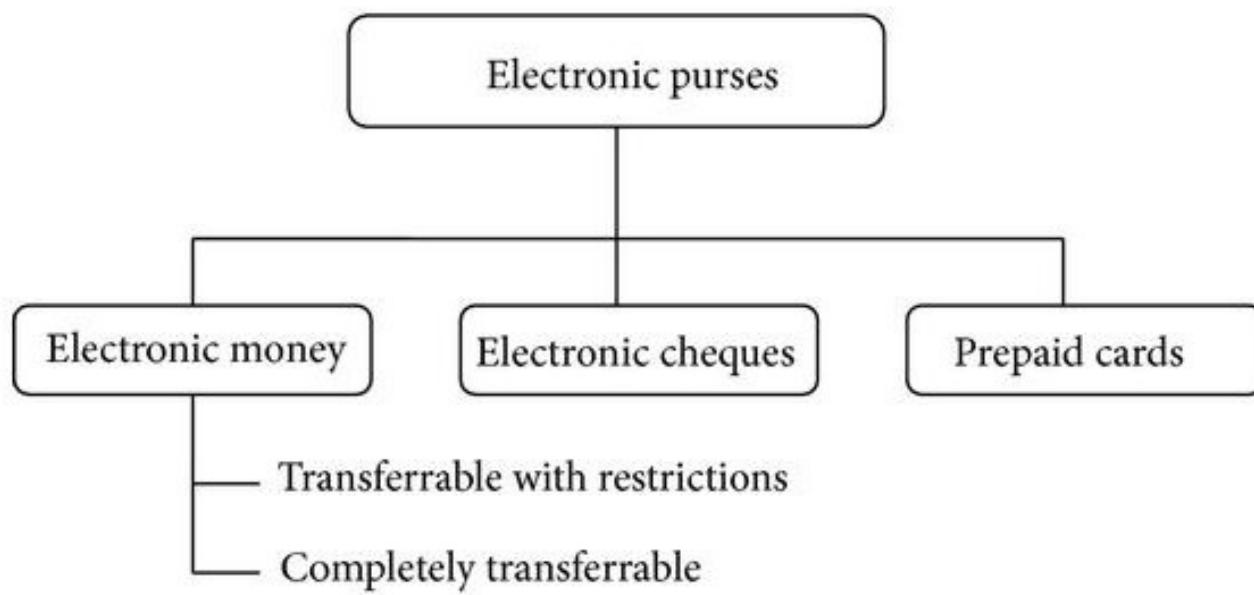
White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as Security Analysts



ELECTRONIC PURSE

The electronic purse, a new payments instrument offering advantages to both consumers and merchants, may soon replace currency in many routine transactions. Widespread use of the electronic purse could, however, raise concerns about consumer protection and the safety and soundness of the instrument.



Types of E wallet

Based on where the information is stored

Server Side Electronic Wallet:

- A server side electronic wallet stores a customer information on the remote server belonging to a particular merchant or wallet publisher

Client Side Electronic Wallet:

- A client side electronic wallet stores customer information on his/her own computer.
- Many of the early electronic wallet were client side wallet that require users to download the wallet software



Disadvantages of E Wallet

- **System Outages:** Information for E wallets are stored on the cloud of business server, therefore the risk of a system malfunction or shut down is always present.
- **Security:** Companies must ensure that their customers' information is encrypted and well protected.
- **Investment:** The initial monetary investment for building a functional E wallet application is quite large as it requires the development of the software as well as continual maintenance.

Compact Embedded Systems

What are Embedded Systems

- An embedded system is a computer system—a combination of a computer processor, computer memory, and input/output peripheral devices—that has a dedicated function within a larger mechanical or electrical system.
- Embedded systems control many devices in common use today.

-
- It is *embedded* as part of a complete device often including electrical or electronic hardware and mechanical parts. Because an embedded system typically controls physical operations of the machine that it is embedded within, it often has **real-time computing** constraints.

Importance and Evolution

- Biometrics refers to automatic identification of a person based on his or her physiological or behavioral characteristics which provide a reliable and secure user authentication for the increased security requirements of our personal information compared to traditional identification methods such as passwords and PINs (Jain et al., 2000).
- Organizations are looking to automate identity authentication systems to improve customer satisfaction and operating efficiency as well as to save critical resources due to the fact that identity fraud in welfare disbursements, credit card transactions, cellular phone calls, and ATM withdrawals totals over \$6 billion each year (Jain et al., 1998).

-
- Furthermore, as people become more connected electronically, the ability to achieve a highly accurate automatic personal identification system is substantially more critical.
 - Enormous change has occurred in the world of embedded systems driven by the advancement on the integrated circuit technology and the availability of open source.

-
- This has opened new challenges and development of advanced embedded system. Since many physiological and behavioral characteristics are distinctive to each individual, biometrics provides a more reliable and capable system of authentication than the traditional authentication systems

Compact Embedded Systems being used

- ATMs
- Fingerprint Reader
- Face recognition
- Signature Verifier
- Voice Recogniser
- Iris Scanners

Fingerprint Sensor(Example)

- Evolution of fingerprint sensing technology. Fingerprint sensors have evolved in two ways. On the one hand, they have become compact in size and cheaper in cost, which makes it possible to embed fingerprint sensors in devices such as laptops or mobile phones.
- While some applications still use a large surface area fingerprint sensor (for capturing a full fingerprint impression resulting in higher accuracy), they are equipped with several advanced functionalities.

EXAMPLE

- A typical example is the slap sensor used in the US-VISIT program [21] , which can capture impressions of multiple fingers simultaneously, thereby facilitating rapid capture of tenprints.
- Other examples include the 3D fingerprint sensor introduced by TBS in 2005 [70] and the touchless fingerprint sensor introduced by Safran in 2010 [26] , which can acquire the images of multiple fingers on-the-fly as the user moves his hand across the device.