Smartcard is a typical plastic card that contains an embedded chip which is either a memory or a microprocessor type, also smartcard can be defined as a device that includes an embedded integrated circuit that cab be either a secure microcontroller or equivalent intelligent with internal memory or a memory chip alone. The card can be connected to a reader with direct physical contact or with a remote contactless radio frequency interface. The following are the environment in which a smartcard can be used in controlling the security.

**Smartcard can be used in securing digital content and physical assets with the organization.**

Smartcard providing information security, smartcards are also used to safeguard services and equipment by restricting access only to permit users. Also in delivering of digital information and entertainment services is encrypted and decrypted via the smart card per of each subscriber base, smart cards have also proved to be useful tools for machine and equipment settings in sensitive laboratories.

**Smartcard used in e commerce or in the issue of financial transaction in controlling security.**

Smartcard facilitate the process of e commerce transaction by enabling consumers to securely store relevant information about purchases for instance the smartcard stores details of personal account like credit balance as well preferences and purchasing trends of consumers. the smartcard can be used for micropayment as well as for management of expenses.

**Smartcard used in various sector like transportation, health in controlling the security.**

Smartcard used in loyalty and stored value in various sectors in which the important information of the people is stored within the smartcard also the payment card to the transportation facilities are the one of the smartcard application for securing the personal information example the smartcard can sometimes use to function as documents such as electronic passport and visas.

**Smartcard used in System boot-up**;

Smart cards can be used for booting personal computers and servers where the system requires critical information contained on the smart card and system startup cannot take place until user authentication takes place. This means that if attackers are successful in gaining physical access to the hardware, they will be unsuccessful in accessing the files.

The resources which can be secured by the smart card are securing the important personal data, securing the physical assets devices like computer system, secure data storage, securing the email content by providing digital signature which validate the email authenticity, secure the digital content.

**Why smartcard suitable for securing the resources**

Because smartcard can provide a higher level of security than magnetic stripe cards as they can contain microprocessor cables for processing data directly without remote connections. When the information is stored on a smart card, it cannot easily be deleted or altered so smart cards are good for storing valuable data.

Also smart card is safe against electronic interference and magnetic fields a multi service smart card can enable user to access more than one different service with just one smart card.

Biometrics are the body measurements and calculations related to human characteristics, biometric is the most suitable means of identifying and authenticating individuals in a reliable and fast way through unique biological characteristics. The biometric security evaluates an individual’s bodily elements or biological data, it is the strongest and most foolproof physical security technique used for identification and verification.The environment in which the biometric can be used in controlling security are.

Biometric used in access control within the organization by using the fingerprint the authentication of the employee can be easily be enhanced through accessing the devices like computers and network facilities within a certain room in which biometric used in doors for authenticate the authorized employees.

Biometric can be used in controlling accessing data as the logical access, through biometric you can control the access of data to the devices such as logging into a device, pc or network the various biometric type can be used in controlling the security to the organization like fingerprint, facial recognition so as to identify the authorized user to the device or network.

Biometric used in register and identify, through biometric like fingerprints, facial recognition you can register a people as employee within the organization so as to make identification easy within that organization, when the registration occurs by biometric you can strong controlling security. Also by using biometric the identification can easily have enhanced for the people.

The resources secured by biometric are the personal information, data, computer systems, networks facilities.

**Why biometric suitable for securing the resource.**

Biometric is suitable for securing resources because of high security and assurance in which it identifies and provide the answers to something a person has and helps verify identity

Biometric is convenient and fast due to user experience also biometric is non transferrable everyone has access to a unique set of biometrics. Biometric like face patterns, fingerprints, iris are impossible to replicate with the current technology.

**References**

Wirt, B. (2003). Biometric system security - Part 2. Biometric Technology Today, 11(3), 8–9. https://doi.org/10.1016/S0969-4765(03)00318-7