Smart card refers to a plastic card with a built-in microprocessor, used typically to perform financial transactions. Smart cards generally look like credit cards. What makes the smart card different from an ordinary plastic card is the technology embedded in it that makes it "smart," provides storage capacity of 1K to 64K and enables it to be used in controlling access by identifying and authenticating the user. In addition to memory or a microprocessor chip, smart cards incorporate RAM, ROM, EEPROM and a serial communications interface.

The environment and applications in which the smart card used in controlling the security;

i. **Financial institutions;** Banks and insurers are using smart cards for electronic payments because of their capability to process data, their portability and tamper-resistance. Stored-value cards (i.e. prepaid phone cards, transportation cards) and cards that access money balances are both gaining in popularity.
ii. **Medical information;** In Europe each individual customarily has a smart card containing pertinent medical information that can be presented to any hospital or doctor from whom the individual seeks treatment. These smart cards can be updated after each treatment before being returned to the patient. They also carry pertinent contact information and emergency medical data.
iii. **Private sector use;** Private sector companies like Microsoft, Exxon, and Pfizer are also issuing smart card IDs, some with biometrics like fingerprints, photos, and facial recognition, to protect their networks and facilities worldwide.
iv. **Physical access;** More and more hotels, corporations, universities, hospitals, health clubs and commercial buildings are issuing smart cards to personalize access. The use of these cards allows the issuer to give or deny access based on privilege and time restrictions.
v. **System boot-up;** Smart cards can be used for actually 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.

Biometrics is a technology for measuring and analyzing biological data of a human body such as fingerprints, eye retinas, irises, voice patterns, facial patterns, and hand geometry, and vascular patterns and DNA. Biometrics is mainly used for authentication purposes. Biometrics technology is used to prevent fraud, enhance security, and reduce identify theft. The environment and applications in which that Biometric used in controlling the security.

The environment and applications in which that Biometric used in controlling the security;

i. **Screen navigation;** One of the most important of people with disabilities is screen navigation. Using cameras, the application can track a person's eye movements in order to scroll a web page, write text, or perform actions by clicking on button on a computer or mobile devices. Therefore, this kind of application is gaining more attention recently due to the rapid development and the growing need of new means of screen navigation especially on mobile devices platform.

ii. **Border control and airport;** A key area of application for biometric technology is at the border. Biometric technology helps to automate the process of border crossing. Also, most international airports have adopted iris, fingerprint, or face recognition systems to prevent terrorists or illegal immigrants entering the country using false identity

The following are the resources that should be secured by using Smart card and Biometric system;

i. Id system

ii. Cardholder

iii. SIM Card Registration

Importance of using the Smartcard and Biometric tools for securing resources in any organizations;

Smartcard;

i. The smart card provides ways to securely identify and authenticate the holder and third parties who want to gain access to the card. For example, a PIN code or biometric data can be used for authentication.

ii. They also provide a way to securely store data on the card and protect communications with encryption.

Biometric;

i. The biometric systems work on the basis of the behavioral traits of the users or the physical traits of the users or a mix of these.

ii. Behavioral biometric systems use methods such as voice recognition, signature verification, keystroke recognition, gait, and so on.

References

Asha, S., & Chellappan, C. (2012). Biometrics: An Overview of the Technology, Issues and Applications. *International Journal of Computer Applications*, *39*(10), 35–52. https://doi.org/10.5120/4859-7134

Martha, E., & Robert, B. J. (1988). *Computer Science and Technology Smart Card Technology : New Methods for Computer Access Control*.

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

Zanero, S. (2002). Smart Card Content Security. *Dipartimento Di Elettronica e Informazione*. http://home.dei.polimi.it/zanero/papers/scsecurity.pdf