CHAPTER II
BASIC THEORY

II.1 Briefly Description : Security System

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organizations of all sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat (Bhatia, 2013).

II.2 Biometric Security

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. The past of biometrics includes the identification of people by distinctive body features, scars or a grouping of other physiological criteria, such like height, eye color and complexion. The present features are face recognition, fingerprints, handwriting, hand geometry, iris, vein, voice and retinal scan. The most recognized biometric technologies are fingerprinting, retinal scanning, hand geometry, signature verification, voice recognition, iris scanning and facial recognition.

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below:

1. Identification (1: n) – One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

2. Verification (1:1) - One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan

Biometric Technology such as: fingerprint recognition, voice recognition, signature recognition, palm scan, iris scan, retina scan, hand geometry, signature scan, keystroke scan and face recognition (Bhatia, 2013).

II.3 Briefly Description : Identification and Authentication

Identification provides user identity to the security system. This identity is typically provided in the form of a user ID. The security system will typically search through all the abstract objects that it knows about and find the specific one for the privileges of which the actual user is currently applying. Once this is complete, the user has been identified.

Authentication is the process of validating user identity. The fact that the user claims to be represented by a specific abstract object (identified by its user ID) does not necessarily mean that this is true. To ascertain that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. Authentication is the process of ascertaining claimed user identity by verifying user-provided evidence

User identification and authentication are typically the responsibility of the operating system. Before being allowed to create even a single process on a computer, the individual must authenticate to the operating system. Applications and services may or may not honor authentication provided by the operating system, and may or may not require additional authentication upon access to them (Havighurst, 2007).

II.4 Face Recognition

In order to recognize a person, one commonly looks at faces, which differentiate one person to another. Face recognition is used to search for other images with matching features. Eyes in particular seem to tell a story not only about which somebody is, but also about how that person feels, where his/her attention is directed, etc. Face recognition records the spatial geometry of unique features of the face. Main focuses on key features of the face. Face recognition technique is used to identify terrorists, criminals, and other types of persons for law enforcement purposes. This is a non-intrusive, cheap technology. In face recognition 2d, recognition is affected by change in lighting, the person's hair, age, and if the people wear glasses, low resolution images

It requires camera as equipment for user identification; thus, it is doubtful to become popular until most peaces include cameras as standard equipment. United States used same technologies to prevent people from obtaining fake identification cards and driver's. Facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. (Bhatia, 2013)

II.5 SWOT Analysis

The SWOT analysis is a business analysis technique that your organization can perform for each of its products, services, and markets when deciding on the best way to achieve future growth. The process involves identifying the strengths and weaknesses of the organization, and opportunities and threats present in the market that it operates in. The first letter of each of these four factors creates the acronym SWOT.

Figure 2.1 SWOT Analysis

The SWOT analysis is a popular and versatile tool, but it involves a lot of subjective decision making at each stage. It should always be used as a guide rather than as a prescription and it is an iterative process. There is no such thing as a definitive SWOT for any particular organization because the strengths, weaknesses, opportunities, and threats depend to a large extent on the business objective under consideration (Team FME, 2013).

.