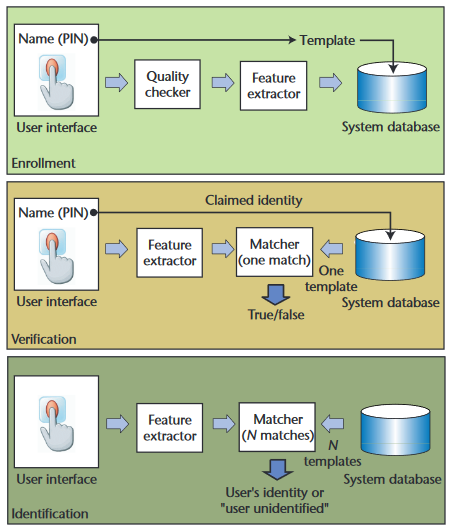
Thomas & Friends CN151/DF151/SS152

**Theoretical Framework & Conceptual Framework**

Access Control

Access Control is the ability of one place or resource to limit access through different media, such as PINs, passwords, biometric scans, etc. Access control runs on comparing data from the database with the current input, scanning for a pair that matches the current input. Access control works at different levels in a system. Access control working at the Application level is based on the users roles, some features are available to higher level roles, and are restricted to those below them. Applications can be written on top of middleware, access control working at the Middleware level is ensures a certain process, usually used in database management systems. Middleware uses facilities provided by the operating system, access control working at the operating system level provides basic security for files and ports. Lastly, the operating system heavily relies on the hardware, access control working at the hardware level controls the memory addresses a process can access (Anderson, 2001).

Biometric Authentication

 Biometric authentication is the process in which physical characteristics are used to validate identity, making it hard to fake and tamper as these attributes are unique to one person only. Physiological characteristics are used in order to authenticate access such as Fingerprints, Palm prints, DNA, iris recognition, etc. The wide use of biometric authentication in the community heavily increased the level of security one device or facility has.

Biometric system can be used in two modes. The first one is the identity verification which occurs when the ide ntity of the user is already enrolled in the system (Has an ID card or login name). The biometric data that is gathered from the user is compared to the user's data that is already stored in the database. The second mode which is the Identification, or also known as search, occurs when the identity of the user is priori unknown. In this mode, the biometric data of the user is compared to all the records in the database, even though the user does not have data stored in the database. It is noticeable that the second mode is more challenging and costly (Enstitutsu).

Fig 1.a: Biometric Authentication Process

Fingerprint scanners needs to fulfill 2 jobs, getting the image of the finger, compares the ridges and valleys of a fingerprint with existing fingerprints. Only unique characteristics are recorded and encrypted. The unique characteristics are then converted into a binary code, and is stored in a database, which are then used to validate entries.

Juels and Sudans Fuzzy Vault Scheme

Fuzzy Vault is an encryption scheme, stating that in order to encode an information, a key is required to decode it with ease. Its concept revolves around the idea that “A secret is encoded using a set values (the key), and can then be unlocked with another set of values if it has fairly large resemblance with set used to lock it”. The Fuzzy Vault is often used with Reed-Solomon codes also known as error-correcting codes. 2 algorithms are used in the fuzzy vault scheme, LOCK and UNLOCK

Capacitive Scanner

Capacitive scanner depicts a picture of friction ridges of a person’s finger through the use of electrical currents. Its sensors are made of semiconductor chips which have arrays of incredibly small cells and each cell of it have a couple of conductor plates protected by an insulating layer. The sensor is attached to an electrical circuit wrapped around an inverting operational amplifier which is basically an integrator. Integrators are complex semiconductor device that performs the mathematical operations.

In order to scan you must have the switch shut first in order to gain neutrality to the integrator circuit, and when it is enabled again, the processor will apply a constant charge to the integrator circuit to have the capacitors charged up. The stored electric charge of the feedback loop’s capacitator influences the voltage at the amplifier’s input which then affects the amplifier output. Afterwards, the scanner processor scrutinizes the voltage of each cell to put together a complete image of the fingerprint.

Access Control

Biometric Authentication

Fuzzy Vault Scheme

Fig 2.a: Biometric Authentication Concept

Access control is the limiting of entry from a certain place or resource, and one type of access control technology is biometric authentication. Biometric authentication is the process wherein physiological attributes are used in order to validate identity. Some of the algorithms used in Biometric Authentication is the Fuzzy Vault Scheme, objects are compared and the state will only change to “unlock” if there are a lot of nuances between those 2 objects.