A growing security issue in ATM machine especially the use of card-PIN method has been of great concern to my researchers because the attacker can easily compromise the machine by using different methods. In view of this, this paper try to see how these problems of Card-PIN can be reduced if not totally eradicated; this paper comprises of the following implementation process: The process of enrolment involve the account holder opening an account and register with the bank of their choice this will enable the bank to have all the enrollee’s information and all necessary details that concern the enrollee and take the biometric data captured of the person that own the account and store in the database, which will be used later for the process of verification and further update of information. The process of extraction and verification make used of minutiae-base techniques. This is to obtain an efficient and thoughtful result in order to reduce or eradicate the problems which is associated with the use of card-PIN and high rate insecurity people faced in using ATM machine.

**ENROLLMENT PROCESS:**

Before an Account holder being identified or verified by a biometric device, the enrollment process must be completed. The aim of this enrollment process is to create a summary profile of the user (Card Holders’). The process consists of the following:

**BIODATA:**

This comprises the Following: Surname, First Name and Last Name which take alphabetic characters, Account Type: Current, or Saving this also take alphabetic characters, picture of the enrollee which can take binary characters, Nationality of the enrollee take alphabetic and string characters, date of birth take string characters and the date account was issue take string characters too. Fingerprint Image Capture: The Account Owner fingerprint will be captured with fingerprint scanner for a minimum of two or three biometric readings, by placing a finger in a fingerprint reader. Not all the samples will be stored; the technology analyzes and measures various data points unique to each individual. The number of measured data points varies in accordance to the type of device. Minutiae Feature Extraction from Image: This is where the minutiae extraction is done and of course processes like binarization, thinning and bifurcation would be done have a perfect minutiae feature extraction from the image.

**THE ENROLLEE STORAGE:**

This has all the details of all the people that have been enrolled and its stores them with the account number. when there is need to view enrollee’s details or make amends this can easily be done with the use of account number to trace individual’s details and it makes the process of verification easier and faster as it saves time figure:1

**IDENTIFICATION AND VERIFICATION PROCESS**

Once the account holder has been enrolled in a system; he/she can start to use biometric technology to have access to his/her account via the ATM machine or related system to authorize transactions. Identification: This is a one-to-many match. The user provides a biometric sample and the system looks at all user templates in the database. If there is a match, the user is granted access, otherwise, it is declined.

**Verification:** This is a one-to-one match it requires the user to provide his/her identification such as a PIN and valid ATM card in addition to fingerprint. The account holder is to establish who he/she is and the system simply authenticates if this is correct. The biometric sample with the provided identification is compared to the previously.

**AUTHENTICATION**

This is the part of the database that allows access into and out of the database, this part monitors the kind of people that uses the database and controls unwanted users and unnecessary logins and access into the database for more secured and protected database environment. For security purposes servers must also address the problem of authentication. In a networked environment, an unauthorized client may attempt to access sensitive data stored on a server. Authentication of clients is handled by using cryptographic techniques such as public key encryption or special authentication servers such as in the OSF DCE system.