Abstract--- In today's technological era, though it has brought in many convenience features, still it suffers with certain security glitches. Keeping in mind, an attempt has been made through this paper to do away with some of the securities of transactionsthrough Automated Teller Machine (ATM) which have been of real concern in the various parts of the globe. The existing designs in the available service points have series of limitations raising points of security. Highlighting a few- Currently the usage of Personal Identification Number (PIN) as ATM user’s verification and identification has been susceptible to accessibility to the unauthorized user is of utmost security lapse, others being misplacement, card swallowing and forgetfulness, leading to eyebrows raised over the machine’s acceptability and patronage. Objective of this paper is attempting to add more security aspects of ATM machines by integrating it with fingerprint module. Particularly this idea provides each customer a unique identity across the banks, and can be used for identification the verification of the account holder.

Keywords--- ATM, Fingerprint, Secugen, Security.

I. INTRODUCTION

A study has been stated in this paper highlighting the added security features in the ATM machines. Financial transactions through the usage of ATM is prone to various forms of fraudulent skills devised by fraudulent to beat the security of the system. The frauds perpetuated showcased as ATM card theft, PIN theft, card reader techniques, PIN pad techniques, skimming, force withdrawals and beyond. So managing the risk associated with ATM frauds as well as keeping in pace in diminishing its impact has always been an matter of concern faced by financial institutions, because day after day fraudulent techniques are in practice with increased occurrences. Though smartcard based password authentication provides two-factor authentication, viz a successful login that requires the client to have a valid smartcard and a correct password or PIN, extending stronger security guarantee than just password authentication.

But then this system too has an disadvantage resulting in failure if both authentication factors are compromised. Stating an illustration—an attacker can obtained the password and the data in the smartcard successfully. Therefore this proposed paper, tries to throw lights on a third authentication factor which can be a some extent to reduce the current lapses in the security system of the ATM. This enhances the security of authentication, incorporating the features of a strengthened and more efficient identity management systems that can deliver what we term “Unique Identity” based on fingerprint.

II. BACKGROUND

The first automated teller machine was first introduced by City Bank of New York in 1960. Then on, specially in the last three decades, consumers have been using ATM to conveniently meet their financial needs, like- making cash withdrawals, debit card cash advances, and check their account balances. At the same time correspondingly there has been a sharp rise in the ATM related crimes too in the recent years, such as tampering with the ATM terminal and stealth of user’s credit card and password illegally by the criminals. Losing user’s bank card and password stealth leads to the criminal withdrawing all the available cash in the account in the shortest time, causing enormous financial losses to customer.

Authentication methods for ATM cards have little changed since their introduction in the 1960’s. Presently, the authentication design involves a trusted hardware device (ATM card), the only means to verify the identity of the user is the cardholder’s Personal Identification Number (PIN). The security lapses are mostly derived from the pitfalls of the magnetic media. Taking this into consideration an attempt has been made to propose a prototype model to add to the security feature making it more trustworthy and fool proof through the introduction of the fingerprint verification scheme to the already existing PIN number to be used to verify the user before he can access his/her account and make the financial transactions.

III. LITERATURE SURVEY

1) Swarna N et.al, proposed a system on HAND GEOMETRY which refers to its geometric structure. This structure includes width of the fingers at various locations, palm, thickness of the palm, length of the fingers, etc. It is related to the fact that nearly each person’s hand is shaped in a different way and does not transform after certain age [1].

a) DRAWBACK: The palm print scanners are usually bulkier and expensive since they need to capture a larger area than the fingerprints scanners.

2) NachiketSainis et.al, put forth a system that provides unique authentication technique using IRIS RECOGNITION. The iris, due to its situation and anatomy, provides several important characteristics which make it suitable for biometric purposes. Its structure is unique, even the two irises from the same person are different.
a) DRAWBACK: Easily obscured by eyelashes, eyelids, lens and reflections from the cornea and this implementation is costlier [2][3].

3) DeepaMalviya et.al, in this article proposed biometric systems where in the general idea is to use FACIAL RECOGNITION to reinforce security. Facial recognition technology is means of biometric identification since the ability to distinguish among individuals is considered natural. One of the main motive is to diminish and tranquilize the effects of attacks to ATM by use of this technique [4][5].

a) DRAWBACK: This has found limited success because it include acquisition environment and facial characteristics changes that effect matching accuracy and the potential for privacy abuse.

4) DaryRam.T.R suggested an embedded FINGER-VEIN system for authentication on ATM network. The proposed system consists of four hardware modules: radio frequency identification system, image acquisition module, embedded main board, and human machine communication module. Finger-vein being hidden inside the human body, is difficult to be duplicated [6].

a) DRAWBACK: There is difficulty of identify vein pattern changing over a time and hardware implementation is high.

5) Jaswinder Singh et.al, proposed VOICE RECOGNITION technique. It is the ability of a machine or program to receive or to understand and carry out spoken commands. It is generally regarded as one of the convenient and safe recognition technique. Voice verification combines behavioral and physiological factors to produce speech patterns that can be captured by voice processing technology [7][8].

a) DRAWBACK: Voice verification is not effective because acoustics and other external disturbances interfere with the process.

6) Sukhdeep Singh and Dr. Sunil Kumar Singlaputforth idea of recognizing people by their EAR which is relatively new class of biometrics. Several reasons account for this trend: first, ear recognition does not suffer from some problems associated with other non contact biometrics ,such as face recognition; second, shape and features of ear are unique for each person and invariant with age and structure of the ear is fairly stable [9].

a) DRAWBACK: Exact ear positioning for scanning becomes a tedious task.

7) Rohit N. Devikar et.al, proposed a system that supports the ATM card scanning along with an OTP. The user may scan his card and login to the system and may view details but is asked to enter OTP as soon as he clicks money withdrawal option. At this stage the system generates one time password and sends it to the registered mobile number. He now needs to enter the OTP in the system in order to withdraw money [10].

a) DRAWBACK: Users may need to increase their access time due to the waiting time of one-time-password to be sent to them via SMS.

8) Olufemi Sunday Adeoye et.al, proposed a SMART CARD which is a card embedded with chip that runs dedicated applications. There is a computer chip in smart card which makes it called ‘smart’. Smartcards are re-usable,store large quantities of data, speed transaction times, identify the card holder, and provide loyalty benefits. One of the most usage of smart card today is ATM card [11].

a) DRAWBACK: If an account holder has multiple cards then it is difficult to remember password for all the cards.

IV. METHODOLOGY

This paper undertakes a primary search into exploring the possibilities of a new system of usage of fingerprints in ATM as an add-in feature of security in verification to avoid the fraudulent techniques that the present ATMs are prone to. The people are very concerned about the safety for their valuables and money is one of them. To adhere to this demand of the customers, old concepts and devices are getting modified as per requirement of the people. In the day to day life people need and seek new security system as money transactions play an important role in the nature of trade and commercial world. So the need of hour is to provide maximum level of security system to cater to the enormous growing banking technology which has changed the way banking activities are dealt with. So we develop to provide the usage of ATM wherein a customer is able to conduct banking activities conveniently and in less time. An ATM is a mechanical system that has its roots embedded in the accounts and records of a banking institution. In the present system of ATM authentication these transactions are insecure.

In the existing system of ATM client authentication, there is a magnetic card reader, client using the ATM, require Bank card and 4 digit PIN which provide customers with the convenient withdrawal and other services. Another newer high-tech method of operating sometimes called card cloning to entangle the installation of a magnetic card reader over the ATM’s card slot and the use of a wireless surveillance camera to find the user's PIN. Real Card data are then cloned into a duplicate card and the criminal attempts to cash withdrawal. Fingerprint verification scheme along with the PIN number is proposed with the idea of overcoming the piracy in money transactions in the above mentioned system. In order to increase the level of security of the ATM networks the use of a biometric technique for verification along with existing PIN has been thought of a solution to decrease the increasing number of frauds. Another advantage is its reach out to the uneducated people in rural areas rendering an easier manner usage and hence increase its popularity.

The Fingerprint is the easiest ‘something you are’ characteristic to capture and process making it more accessible application. It is time tested and successful. Fingerprinting is one of the most mature technologies and considered legitimate evidence in courts of law all over the
world. It is also used in forensic investigations. Recently, an increasing number of civilian and commercial applications are either using or actively considering using fingerprint based identification because of a better understanding of fingerprints and furthermore, its matching performance is better than any other existing biometrics technologies. A fingerprint is believed to be unique to each person and also each finger. It is unique in terms of the arrangement of its minutiae. Even identical twins have different fingerprints and they do not change over time.

Fingerprint usage is widely accepted by the public, convenient and reliable. Moreover this consumes less time and effort to acquire one’s Fingerprint. Its recognition is considered among the least intrusive of all biometric verification techniques.

There is a wide range of security products available from various companies that revolve around fingerprint-based user identification. A variety of products are available from companies such as: Verification, Digital Persona, SecuGen and etc. For this project we make use of one of the SecuGen products - Hamster Plus. SecuGen Hamster Plus can be used for authentication, identification and verification functions that let your fingerprints act like digital passwords that cannot be lost, forgotten or stolen. We chose this fingerprint scanner over others because of the following features it possesses:

1) High-performance, maintenance-free optical fingerprint sensor.
2) Sensor resistant to scratches, impact, vibration and electrostatic shock.
3) Auto-On (Automatic Finger Placement Detection)
4) Smart Capture (Automatic Image Adjustment)
5) USB connection.
6) Removable weighted stand.
7) Compact, lightweight and portable.
8) Integrated finger guide.
9) Readily accessible for any finger.

Our system integrates biometric identification module into normal, traditional authentication technique use by electronic ATM machines nowadays to ensure a strong, unbreakable security and also non-repudiate transactions. In order to demonstrate the strength of proposed authentication protocol using the combination of two authentication methods of PIN and fingerprint, the proposed design involves two phases namely Registration phase and Verification phase. Each of the phases is briefly described below.

The first being Registration Phase which is carried out prior to identification and verification by a biometric device. This creates a profile of the user. the administrator of the system carries out this process consisting of the following steps:

1) Sample Capture: The user allows any number of biometric readings by placing a finger on a fingerprint reader. The quality of the samples, together with the number of samples taken, will influence the level of accuracy at the time of validation. The technology analyzes and measures various data points unique to each individual. The number of measured data points varies in accordance to the device.

2) Conversion and Encryption: The individual’s measurements and data points are converted to a mathematical algorithm and encrypted. These algorithms are extremely complex and cannot be reversed engineered to obtain the original image. This template is further stored in the database.

3) Identification and Verification: Once the individual has been enrolled in a system, he/she can start to use biometric technology to have access to his account via the ATM machine to authorize transactions. Identification: 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: a one-to-one match requiring the user provides identification to PIN and the biometric sample. In other words, the user is establishing who he/she is and the system simply verifies if this is correct. The biometric sample with the provided identification is compared to the previously stored information in the database. If there is a match, access is provided, otherwise, it is declined. After the verification process, the user can carry on with his/her transactions such as balance inquiry, balance withdrawal, balance transfer etc.

V. PRINCIPLES

Summarization of the implementation steps are as follows:

1) A user presents new fingerprint sample information to the biometric system through the sensor.
2) The client processor processes the fingerprint together with the name and identification number and then encrypted and is sent it to the relevant database.
3) The server side processor then queries the database with the sample name and identification number.
4) At the server side processor, the supplied information is decrypted and processed.
5) The requested templates are supplied. The processor now uses a biometric matcher to compare the sample and all templates associated with the user for similarities.
6) The matcher returns a match score representing the degree of similarity between the closest template and the sample.

VI. CONCLUSION

This proposed system is a benefit for both banks and customers in terms of safety and provides a highly secure and effective replacement for ATM Cards. Fingerprint Identification system offers greater authentication and convenience that helps to reduce many issues for avoiding the fraud in ATM system. In addition to this, solution provides a high level of assurance users of a system are who they say they are. The fingerprint module is chosen for it’s coding versatility, friendliness and compatibility. The proposed system is cost-effective and much secured and will reduce the ATM machine theft if not totally eradicate theft associated with the use of ATM machine.
VII. Future Scope

The scope of the project can include the following:

1) The ease of access, i.e in case of emergencies other person than the account holder should be able to carry out transactions.
2) For this, at the time of enrollment, a nominee’s fingerprint sample can be taken and stored in different column at the database.
3) The nominee can carry out only a limited number of transactions.

References


Aishwarya Kulkarni, B.E, Computer Science and Engineering, Vijayapur, India. E-mail: aishwarya. (E-mail:kulkarni46@gmail.com)

Ria Jain, B.E, Computer Science and Engineering, Vijayapur, India. (E-mail: riajain@gmail.com)

Archana Reddy, B.E, Computer Science and Engineering, Vijayapur, India. (E-mail: archuredy@gmail.com)