I. INTRODUCTION
In the war of functionality versus security, the functionality wins more often. Security has always been viewed upon as an overhead or afterthought by software developers. But in the case of banking and money transactions, the security should hold highest priority. Increase in daily attacks on ATM and banking security the developers getting on right track and putting security their important aspect in developing projects. The multifactor authentication is an approach to authentication, which requires the presentation of two or more authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). After presentation, the other party for authentication to occur must validate each factor. In present days the ATM holds only one thing (i.e. PIN) to secure the money saved in the bank if we are not considering the physical attacks. In our system, we are going beyond this level of security to enhance security of the ATM. We introduce the concept of one time password (OTP) in ATM banking. Our system will provide the second level of security using different factors to generate OTP. This will send over customer’s mobile number stored in records. In secure ATM, user will have to register mobile and its IMEI number in bank system. When user puts/swipes card into machine, user get request to insert PIN (which is current way of ATM banking). In the proposed system user will get OTP on mobile. When user enters OTP to the system, he/she will be having access to the machine else no transaction can be made.

II. LITERATURE REVIEW
A Novel Method to Enhance the Security of ATM using Biometrics.
Nowadays we are using the pin number for security in ATMs, which replaced signature-based system. The pin based security is the simplest level of security. The pin number is a unique number, which is encrypted and decrypted during transaction. Nowadays the pin number can be extracted through many ways, for fraudulent activity. So, as a solution the pin number can be replaced with biometric security. The biometric security may be fingerprint, retina and so on. Nowadays, the system is used to compare the input image with the image in the database and if they are verified, the bank staff would disperse the cash. But
the proposal model would completely replace the pin number with biometric system and the machine would disperse the cash when the comparison gets satisfied. Thus the security of the transaction is improved to a greater extent.

Biometrics to Control ATM Scams: A Study In the current scenario the way banking and transaction system is changing in the world, the validation, authentication and confirmation of a person is very important and should be of more concern. Authentication and verification has always been the part to worry about the security and confidentiality of the consumers. In the rapid changing environment it’s not easy to maintain integrity and authenticity of persons. There is a lot of risk to losing money and identity if we lose our ATM PIN. If it is hacked by someone then we can lose entire money. To prevent all these frauds we need some foolproof security solution which we can use along with the current available technology. Biometric is one of the technologies which we can combine with the current technology. We can use fingerprints, iris scan, palm scanning along with the PIN authentication and verifications. Even we can use voice recognition also. Combination of such technologies may help in reducing the ATM frauds and hence can improve the security level of other financial transactions.

Smart atm security system using fpr, gsm, gps

This paper gives the description of the new approach towards the security of ATM (Automatic Teller Machine) systems. The objective of the paper is to know the Enhanced smart ATM security system which is developed using the Embedded system and advanced technologies. In our proposed system RFID card is used as ATM card, IR sensor in order to sense the presence of the card holders and to turn on Fan and Light, if ATM is tampered then SMS is sent to two main stations via GSM. GPS is used to track the location in case the cash box is robbed. Finger print is used to identify and verify authorized bank personnel. Hence the proposed system is the highly secured system for ATMs.

Fingerprint and Iris Biometric Controlled Smart Banking Machine

This paper describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint and iris authentication. system provides protection to the ATM terminal from fire and thief attacks by making provisions of pump motor and a DC motor for rolling the shutter.

III. IMPLEMENTATION

Existing process

There is no security layer is implemented in the ATM card except PIN number. It is very costly to include fingerprint and Iris scanner in normal transaction. ATM card falling into wrong hands, and the PIN number being cracked by a stranger. Then stranger can easily use the ATM card. It is possible that the machine is tempered and read wrong information as correct information. It is also possible that the magnetic strips hold legitimate information but that card is duplicated. PIN can be hacked by any means like shoulder surfing, mutual friends, family friends etc. After PIN is correct, there is no one who can catch attacker to steal money from bank. It is just like stealing from cupboard.

Proposed methodology

All these factors are verified for the authentication purpose of the user along with atm scanning and biometric verification. If any of the above said, parameter are differing and then the link is generated to the User’s Mobile number for further more secure authentication system. In the modification phase, an automation user Internet (Bank server) recognition model using mobile is designed to enhance the user comfort and detection of the time span spend by the user in the ATM machine. The system improves the security of ATM’s. Use of Biometric and link provides second level of security. The system is cost effective and cheaper than usual ATM systems.
Admin mode: In this mode the user fingerprint and mobile number are collected and saved at the time of opening the account.

User mode: In this mode, the user fingerprint is validated with saved fingerprint for the identification, which is required to perform transactions. This software system is designed as follows: In next step, the system is initialized to check specific task, such as checking ATM terminal, GSM module and so on, and then each module is reset for ready to run commands. Before accessing ATM system, the mobile number and fingerprint of the customer are needed to be authenticated.

IV. CONCLUSIONS
The system also contains the original verifying methods which was inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the fingerprint technology which makes the system more safe, reliable and easy to use. As we know that fingerprint are the most acceptable biometrics all over the world in identifying a person. Some government in the world are still implementing fingerprints technique to identify their citizens and the criminal from the scene of crimes in forensic work.

Future enhancement
Many criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bankcard is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he and she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is non-transferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. This technique is very useful in future for avoiding the fraud in ATM system.

REFERENCES