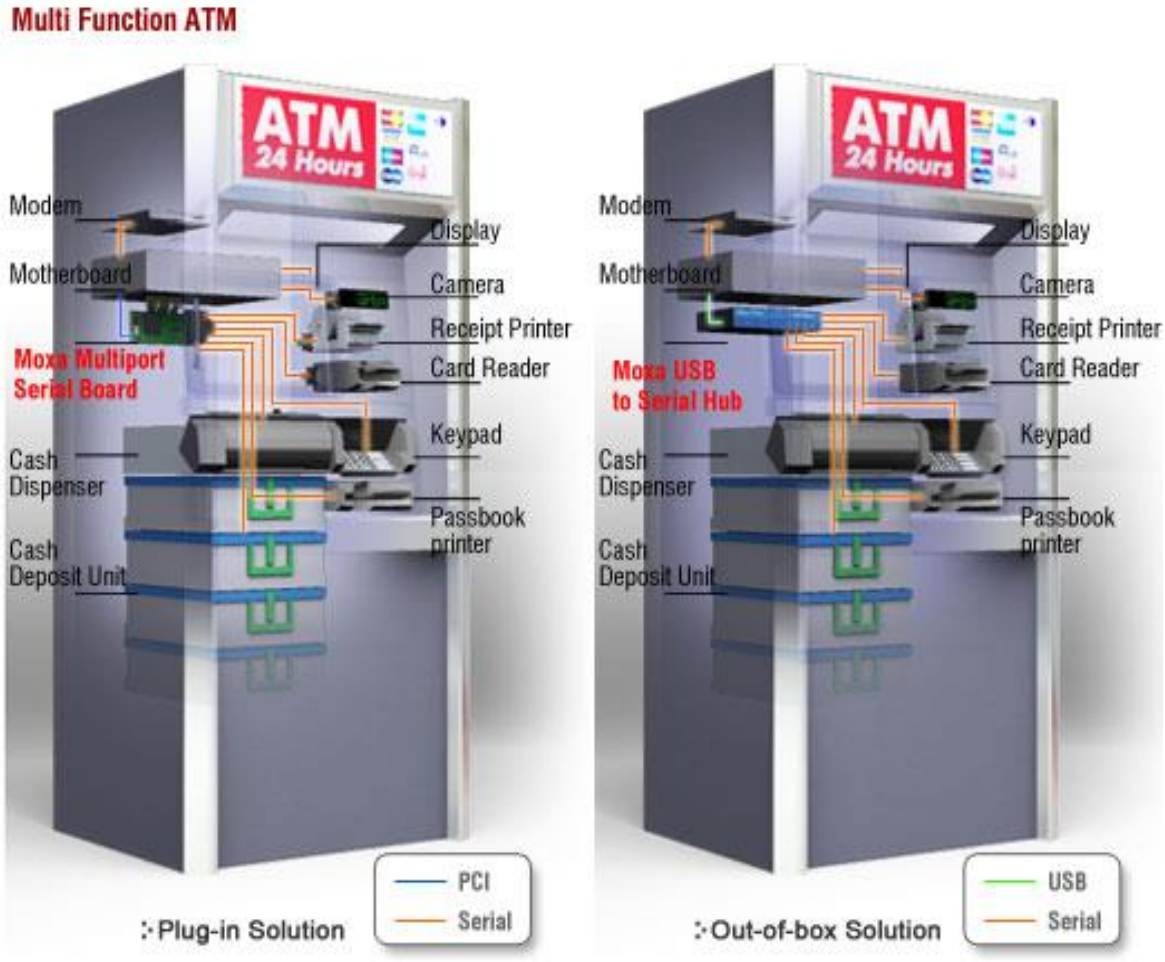
ATM Security

Kavita Hooda

Abstract- ATM is an automated teller machine which is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. In ATMs the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip (that contains a unique card number and some security information). The first ATM was installed in Enfield town in London on June 27, 1967 by Barclays Bank. ATMs are known by various other names as Automated Transaction Machine, Automated Banking Machine, Cash Point(at Britain), Hole in the wall, Ban comet(in Europe and Russia) and Any Time Money(in India)

Index Terms- Skimmimg, Biometric, database, Decomposition, User Case Diagram, Simulator and state chart.



I. Introduction

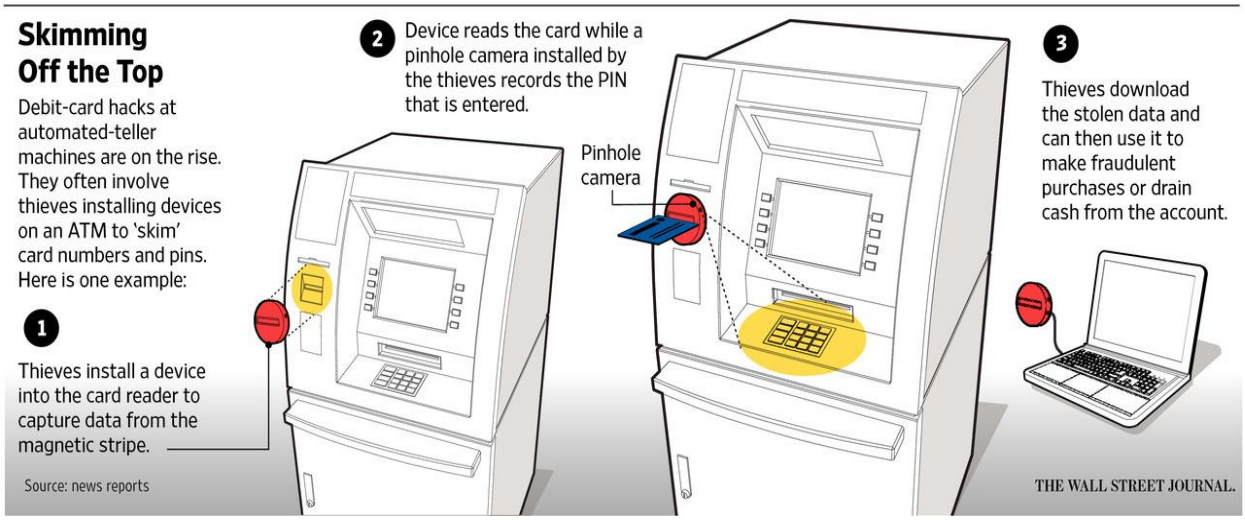
In modern world, numerous of people are dependent on computers for keeping major record of data. Data are transferred in a cost-effective manner across wide area. ATM is one of the automatic systems being used since 1967 by many of us. ATM was invented by John Shepphardbaren on June 1967 at United Kingdom. It first came in India in 1968. Today, many people have PIN's and password for operating multiple devices like car, mobile, ATM machines ; herein using PIN's without safety results in a major difficulty faced by customers like usability, memorability and security. Some people used to write their PIN and password on some paper or diary which is not at all secure. As, it can be easily attacked and hacked by someone, resulting the account holder can suffer.

With the growing sector of banking, everyone is using ATM machines as these machines are located in different places and the customer can access his account anytime anywhere.

A customer holding a bank account can access the account from ATM systems by getting a PIN or password confidentially

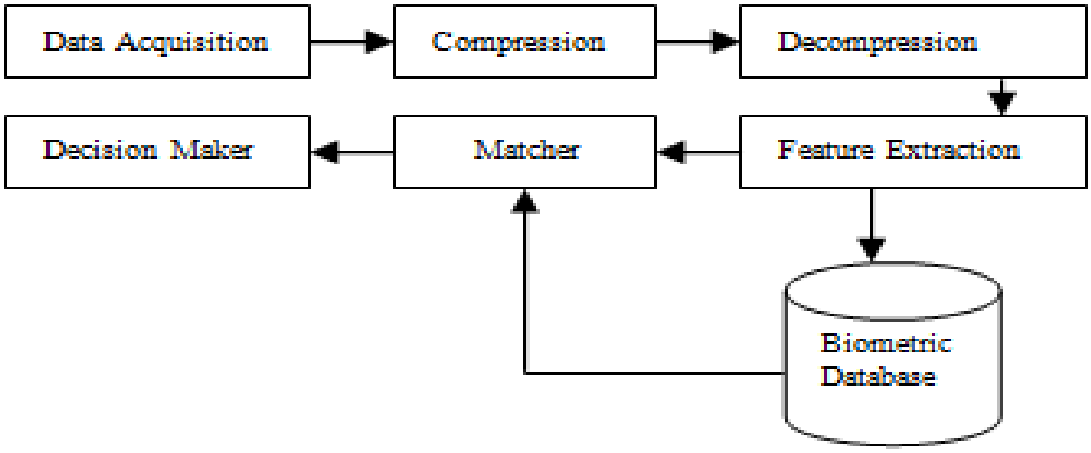
from bank. By scratching the ATM card into the machine and entering PIN number, one can easily perform transaction, transfer money, etc. PIN number is a crucial aspect used to secure information of customer's account, thus should not be shared with others.

In this regard, an intuitive approach is to introduce biometric authentication technique in ATM systems, i.e., face recognition technique from 3 different angles using high resolution camera. Although various biometric technique like- fingerprint, eye recognition, retina and iris recognition, etc have been devised as an authentication method for ATM machines, still there is need to enhance the security in ATM systems to overcome various challenges. This paper focuses on security of ATM system i.e., how to augment security of transaction using face recognition from 3 different angles at a time. The study aims to design a module of an ATM simulator based on face recognition from 3 different angles in order to minimize frauds associated with use of ATM systems.



II. BIOMETRIC

The word "biometric" is a Greek word that is derived from 2 words- bio (life) and metric (to measure). Biometric can be stated as measure of behavioral and physical characteristics that are captured and stored in database and further compared with an instance for verification purpose.



Here, Data acquisition, compression, decompression, Decision Maker, Matcher terms are used to provide security by

using Biometric database which stores the necessary elements and information for security.

III. LITERATURE REVIEW:

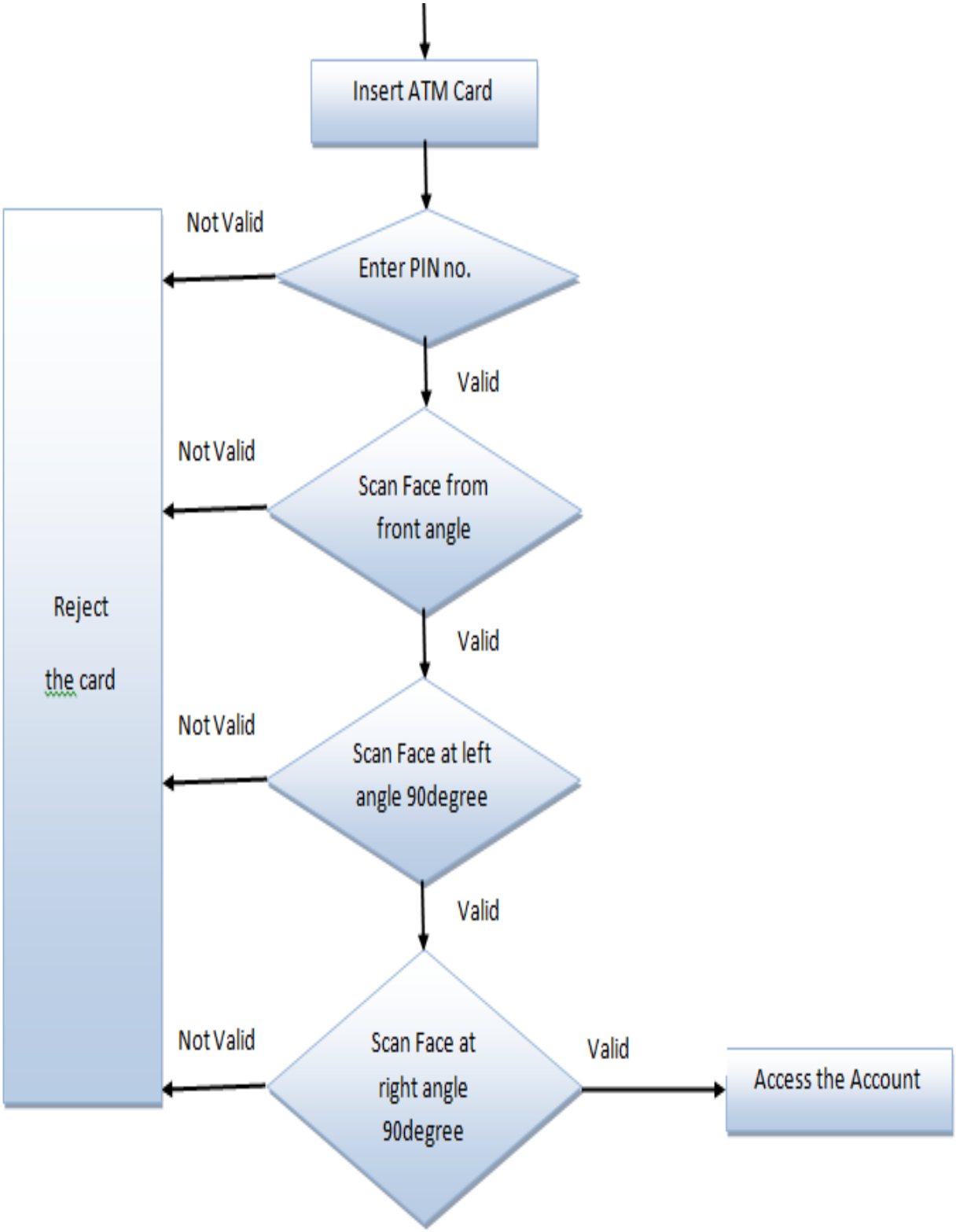
Security Experts says that Automatic Teller Machine (ATM) in future will have biometric authentication techniques to verify identities of customer during transaction. In South America, there are companies that have introduced fingerprint technology as a embedded part of ATM systems, where citizens have already started using fingerprint in place of PIN or Password for general identification with their ID cards. Gregg Rowley said- "Banks will move to smart cards and biometric will be next step as fingerprint verification and face identification technique. Bank has already been moved to smart cards and now is the time to implement biometric authentication approach in ATM systems.

Nowadays, there are devices to perform biometric identification and authentication of following: fingerprint, hand, retina, iris, face, and voice. Rowley says,"Most insecure is a magnetic stripe with a PIN, more secure is a smart card with a PIN, and even more secure is a smart card with biometrics. India is still lacking in implementing biometric with smart card as a safety approach. Various ideas are given by researchers for biometric authentication including- fingerprint, iris and retina, voice, etc. Fingerprint approach for identification given by Oko S. and Oruh J. (2012) not proved efficient as when citizen will move to ATM system, fingers may become dirty from natural environment and will not be able to access his account with ATM system, since fingerprints will not match from the one that was traced during identification. Secondly, a iris and retina approach proposed by Bhosale S. and Sawant B.(2012) as a identification method, but citizens might not want a laser beamed into their eyes for retina scan at every time he wants to access account through ATM. Thus, iris and retina as identification authentication proved inefficient. Vibration detector sensors were also proposed as a security system for ATM machines by Ajaykumar M. And Bharath Kumar N.(2013). Voice was also proposed for security in ATM systems as a biometric with smart card. The cons were there at the same time as two citizens can have same voice and one can easily hack and can fraud with another's account. Thus, this paper came with an idea of face recognition technique with 3 different angles as a biometric authentication that cannot be lost, stolen, harmful, dirty, copied, forgotten and is always available. Thus, biometric device is ultimate attempt in trying to prove who you are.

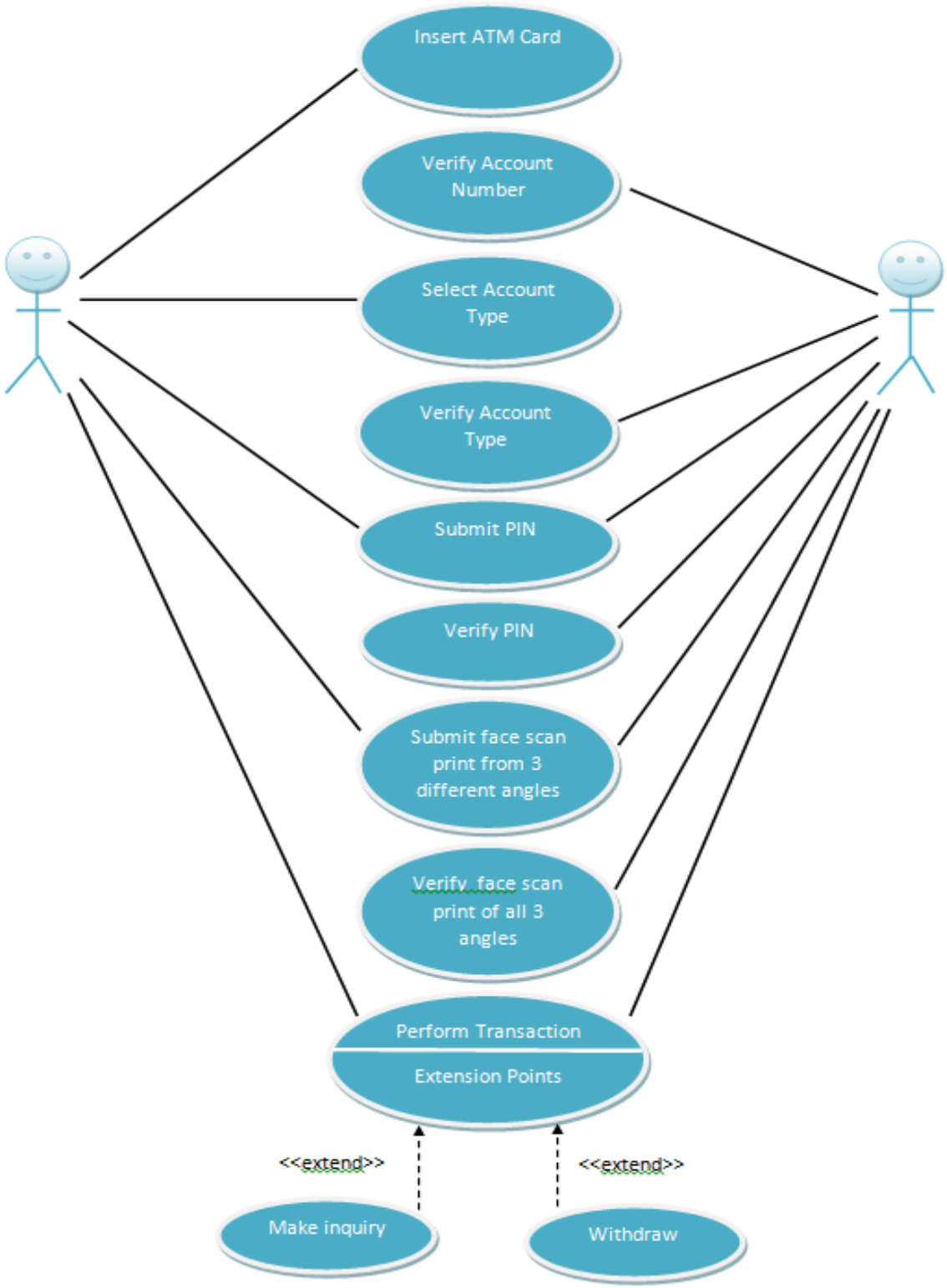
IV. DESIGN METHODOLOGY:

Face Recognition is a biometric scan technology. Face Recognition includes face scan system that can range from a high-resolution camera, workstations, software and back-end processors. Face scan technology is used to analyze and capture facial characteristics such as distance between eyes, mouth or nose, and face cut of person. The ATM system will consist of embedded camera in machine that will recognize the face standing about 2 feet far in front of system and perform matches against the facial database. The system will usually come to a decision in less than 5 seconds. It is very important that the face is at proper distance from camera or system, at proper angle and lighting is appropriate, otherwise distance from camera will reduce facial size and thus resolution of image. Facial-scan technology has unique advantage, over all other biometrics in the area of surveilling large groups and the ability to use pre-existing static image.

Biometric device works in order to capture human characteristics, such as fingerprint, iris and retina, voice and face. Many devices are there that can be used for biometric authentication like hand print detectors, voice recognizer, high resolution camera and identification patter in the retina.



System Flow Diagram for ATM using Biometric



Use Case Diagram for ATM Simulator

In working of Biometric authentication, a database is maintained by banks in which sample of user's characteristics are stored as identification information. Thus, while using ATM system, during authentication, the user is required to provide another sample of the user's biometric characteristics. The below diagram represent the details as

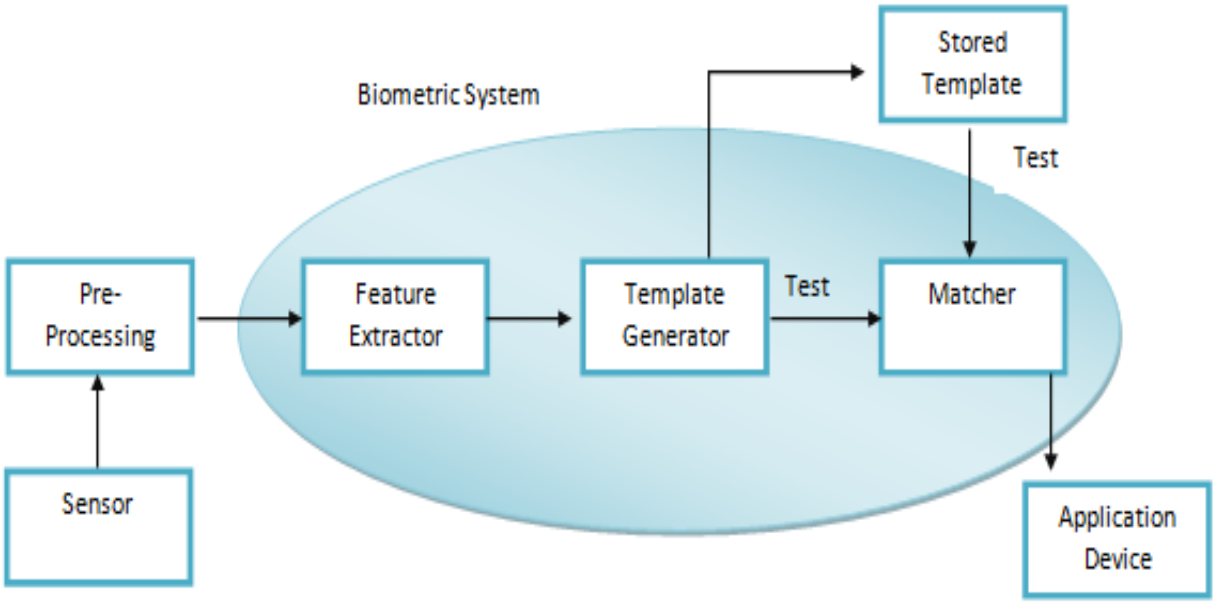


Fig. Working of Biometric Authentication

Biometric Authentication process involves: the matching of extracted feature with the sample feature already stored in database. When user provides a sample of same nature i.e., face scan etc. with its PIN in ATM system, then the system sends grid points of user's face to database as algorithm of numbers through a network to server. On server side, the user's current sample is matched after decryption and compared with the one stored in database. As soon as, the sampled images match the current image, the user is allowed to proceed further as an authenticated user for transaction, deposit, transfer, etc., else user is considered as invalid user and session is terminated.

Working of ATM system with biometric authentication can also be explained using state chart diagram. It shows the state in which an ATM system can be at any point in time. The diagram depicts the flow from one state to another with conditions denoted with arrows.

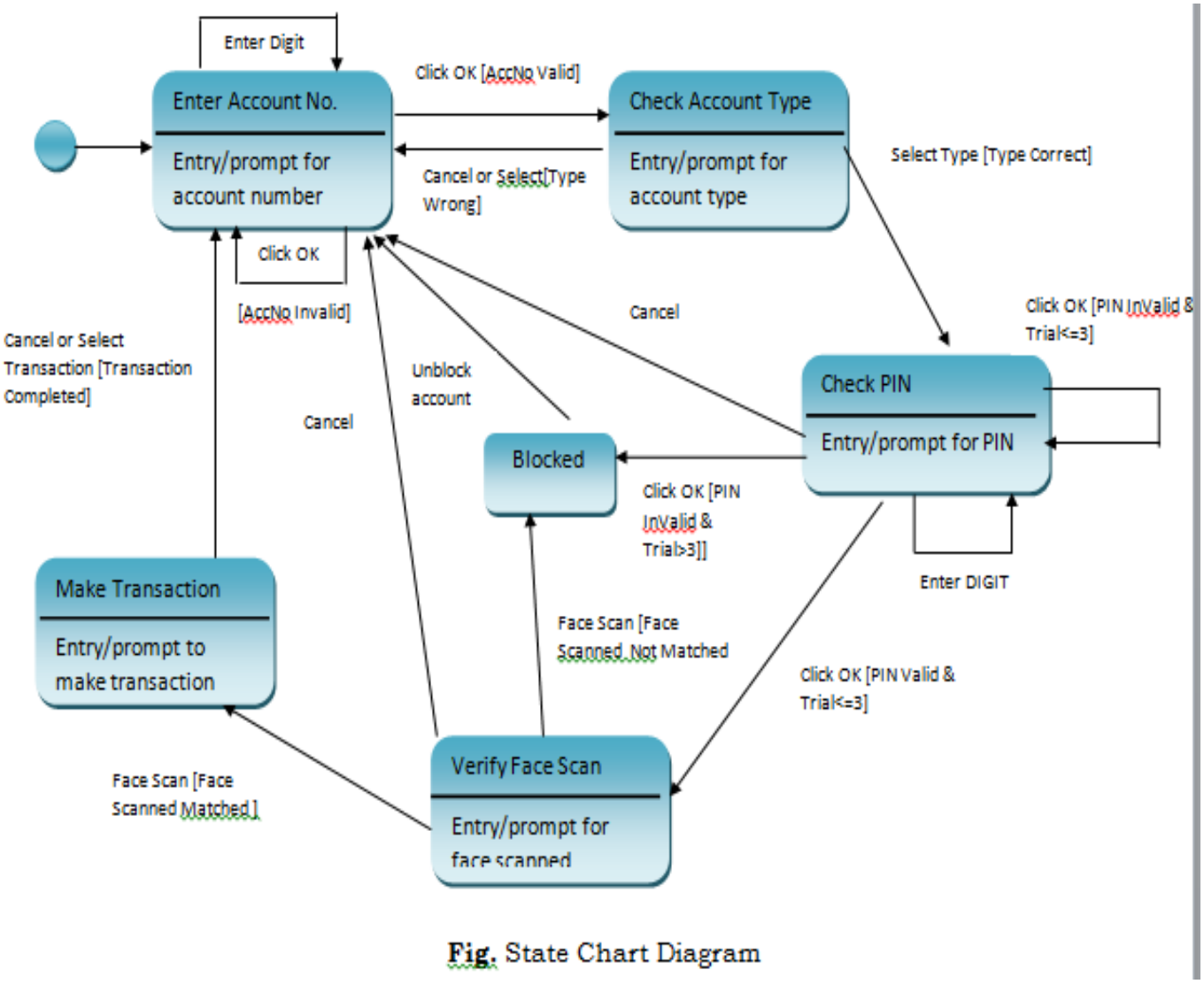


Fig. State Chart Diagram

V. Conclusion

From the above proposed conceptual model, it has been concluded that biometric ATM systems is highly secure as it provides authentication with the information of body part i.e., face recognition from 3 different angles. Biometric Authentication with smart cards is a stronger method of authentication and verification as it is uniquely bound to individuals. It is a viable approach, as it is easy to maintain and operate with lower cost. In this paper, a new authentication technique for ATM system is introduced for secure transaction using ATM's. Devising a face grid algorithm and an effective ATM simulator forms the main focus of our further research.

References

[1] Archana et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(10), October - 2013, pp. 261-266

[2] S.T. Bhosale and Dr. B.S.Sawant "SECURITY IN E-BANKING VIA CARD LESS BIOMETRIC ATMS", International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012

[3] Sunil Lohiya "Biometric identification and verification techniques -A future of ATM Banking System", Indian Streams Research Journal, Volume 2, Issue. 7, Aug 2012

[4] Biswas S., Bardhan Roy A., Ghosh K. And Dey N.,"A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

[5] Zahid Riaz, Suat Gedikli, Micheal Beetz and Bernd Radig "A Uni_ed Features Approach to Human Face Image Analysis and Interpretation", 85748 Garching, Germany

[6] Edmund Spinella SANS GSEC," Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", San Francisco, 28 May 2003

[7] Aru, Okereke Eze, Ihekweaba Gozie," Facial Verification Technology for Use In Atm Transactions", American Journal of Engineering Research (AJER), Volume-02, Issue-05, pp-188-193

[8] Prof. Selina Oko and Jane Oruh, "ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012

[9] M. Pantic and L.J.M. Rothkrantz," Facial gesture recognition in face image sequences: A study on facial gestures typical for speech articulation", P.O. Box 356, 2600 AJ Delft, The Netherlands

[10] http://australianit.news.com.au/articles/0,7204,5633467%5E15397%5E%5Enbv%5E,00.html

AUTHORS

First Author – Kavita Hooda