**LITERATURE SURVEY**

The word “biometrics” derived from the Greek words “bios” and “metric” which means life and measurement respectively [3]. To implement this concept, we have studied different investigated works and found following data. Most finger-scan technologies based on minutiae. The downside of pattern matching is that it is more sensitive to the placement of the finger during verification and the created template is several times larger. For fingerprint recognition, a system needs to capture fingerprint and then follow certain algorithm for fingerprint matching. This research paper discusses a minutiae detection algorithm to showed key parameters of fingerprint image for identification. The maturity of Biometric techniques and generally the dramatic improvement of the captured devices have led to the proposal of fingerprinting in multiple applications but in the last years, minutiae have been the main type of algorithm used. The minutiae are relatively stable and robust to contrast, image resolution and global distortion as compared to other fingerprint representation [4]. Biometric data separated and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information. They cannot be stolen and used to access personal information to solving the bugs of traditional identification methods the author of designs a new ATM terminal customer recognition system is used for the core of microprocessor and an upgraded enhancement algorithm of fingerprint image intensify the security of bank account as well as ATM machine. For image enhancement, the Gabor filter algorithms and direction filter algorithms are used [5]. Miao et al proposed the Gabor filters (GFs) play an important role in the extraction of Gabor features and the enhancement of various types of images. Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest [6]. If images of fingerprint are shoddy images, they result in missing features, leading to the degrading performance of the fingerprint system. Hence, it is very important for a fingerprint recognition system to evaluate the quality and validity of the captured fingerprint images. If Authentication Failure then it send the alert message to the Account holder and Bank [7]. To have good process of operation for fingerprint matching, in depending on the spectral details features two feature reduction algorithms given the Column Principal Component Analysis and the Line Discrete Fourier Transform feature reductions. It can perfectly compress the template size with a reduction rate of 94%. Spectral minutiae fingerprint recognition system shows a matching speed with 125000 comparisons per second on a PC with Intel Pentium D processor 2.80GHz, 1GB of RAM. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they not be stolen and used to access personal information [8]. Fingerprint records usually extend to impressions on the last joint of the fingers and thumb, to the extent that fingerprint cards typically record parts of the lower finger areas of the fingers [9]. Among those new technologies for dealing with payment processing, biometric payment technology has recently attracted more and more attention as a viable solution to decrease identity theft [10]. It may be historical, current or theoretical. The underlying principle of electronic money involves the use of computer networks such as the Internet and digital stored value systems. Examples of electronic money are bank deposits, electronic funds transfer, direct deposit, payment processors, and digital currencies. Electronic money can be understood as a way of storing and transmitting conventional money through electronic systems or as digital currency, which varies in value and is tradable as a currency in its own right [11]. Electronic money transfer at an ATM is a cash equivalent device that is stored on an electronic or remote device in the security of the server and can be described on the one hand as policies, guidelines, processes and procedures necessary to enable electronic transactions to be performed with minimum risk of penetration or intrusion or theft. On the other hand, electronic security is any tool, method or process used to protect system information assets. Information is a valuable strategic asset that is managed and protected accordingly. This insurance is a risk management or risk mitigation tool, and appropriate safety measures mitigate the risk of underlying transaction commensurate with its value [12, 13].

Ratha et al. [15] said biometric authentication become more and more popular in the banking and finance sector [15]. It provides easy to withdraw or do any type of transaction. So all the customer prefers for do transaction in ATM. The idea of fingerprint is not only for security but also to overcome the lack of customer understanding on ATM concept. By this biometric system, illiterate people can also do their transaction with the help of fingerprint. The proposed method needs ATM with biometric, fingerprint security system, in order to meet its customer’s ‟who many of them have savings account and need to have access to their money during non-banking”. ATM with fingerprint scanner offer excellent security to customer since there is very low possibility of fraud. By using fingerprint recognition customers are more comfortable with the idea of saving their money with the bank because they understand that no one can replicate their fingerprint and take their money. Fingerprint authentication is the most popular method among biometric authentication, fingerprint based identification is one of the most mature and proven technique [15, 16]. It provides more security than normal security in the banking system. Biometrics holds the promise of fast, easyto-use, accurate, reliable, and less expensive authentication for a variety of applications [17]. Iwasokun et al. [19] said customer able to do their transaction quick and safe. Because when the entire customers want to deposit cash or withdraw their money, they all want to do their transaction immediately. So all are trying to save their time. Therefore, that bank introduce Automatic Teller Machine (ATM) instead of teller. This machine provides all facility like teller in the bank.

Moreover, it provides better and quick process. Customer does not want to wait in the queue to do their transaction. At the time of transaction customer’s enrol their fingerprint to a high resolution fingerprint scanner. The fingerprint image transmitted to the central server via secured channel. At the banking terminal, the minutiae extraction and matching performed to verify the presented fingerprint image belongs to the claimed user in bank database. The function of the feature extraction module is to extract the feature set from the scanned biometric data. This feature set is then stored into the template database. The matcher modules take two inputs, i.e., feature set from the template database and feature set of the user who wants to authenticate him/her and compares the similarity between the two sets. The last module, i.e. the verification module makes the decision about the matching of the two feature [18], [19].