Prevention of Payment Card Frauds using Biometrics

Ashutosh Singh, Ranjeet Srivastva, Yogendra Narain Singh

Abstract**:** ***Digitization era has paved the path for digital economy. The advent of plastic cards such as credit and debit cards facilitate many services and products anytime and anywhere but they suffer with fraudulent attacks. This paper proposes a novel approach for the prevention of payment card frauds using biometrics. The approach works with the existing payment card security system and takes the advantage of biometric recognition technology that serves with a unique ID and bears an individual's biometric data like Aadhaar. The integration of biometric verification system with the payment card security system not only strengthens the security of card users but also it ensures the physical presence of card holder at the point of sale. The system like Aadhaar may be successfully linked with the payment card processing system for supplementing identity verification of users and making the environment free from card frauds. The performance of the proposed payment card security system using biometrics shows that the probability of breaching user's identity is significantly low and found to be in the range of 10^{-17} to 10^{-20} for face, fingerprint and iris recognition.***

Keywords: Digital Economy, Payment Card Fraud, Biometrics.

I. INTRODUCTION

The payment cards are the plastic cards used to make transactions for electronic fund transfer and access ATMs. Some commonly used payment cards are credit cards, debit cards, charged cards and ATM cards as shown in Fig. 1 [2]. The protocols used by payment cards e.g., card number, size, data formats, flexibility, location of the magnetic stripe, magnetic characteristics, are decided by International Organization for Standardization standards, ISO/IEC 7810-13, 4909 and ISO 8583 etc.

The payment card users are growing exponentially around the world thus raising the cases of fraud committed by identity theft [23]. The cases of stolen card may occur that can be reported by a user for identity theft before its fraudulent use. The study of Federal Trade Commission of United States has shown that the card theft cases are increased by 21% in the first decade of 21st century [18]. The emergence of the payment card security technology like chip-and-PIN by 2010, the payment card frauds are reduced to 0.1% [21]. However securing of payment cards is still a challenge due to proliferation of digital economy and its diverse societal applications.

Fig. 1. Payment cards in use.

A. Digital Economy

Digital society is a term used widely for digital economy that refers to the economic activities facilitated by digital technology [8]. The rapid growth in information, communication and web technologies is made possible the activities of digital economy in the past two decades [15]. This is a new type of economy where computing devices like laptops and mobiles along with networking infrastructure, provide a global platform among people and organizations to fulfill their economic need [17].

Digital economy has grown exponentially and being accepted globally. The Accenture report has shown that the global volume of digital economy would reach to $100 trillion in next couple of years [13]. According to Forbes, 125,000 large organizations have started business initiatives that would increase the digital revenue to 80% by 2020 [34].

Nevertheless, the digital economy is synonymous with digital currency. Digital currency is a currency in digital form and the plastic money is one of the most accepted alternatives present against the traditional payment system [37]. Cards are useful since they are convenient to the users as well as widely accepted by sellers and merchants [24]. It is estimated that around 10,000 transactions are made through cards around the world every seconds [31].

The Federal Reserve payment study shows significant growth in debit card payments between 2012 and 2015 [40]. During this period, the value of payments using both prepaid and non-prepaid debit cards

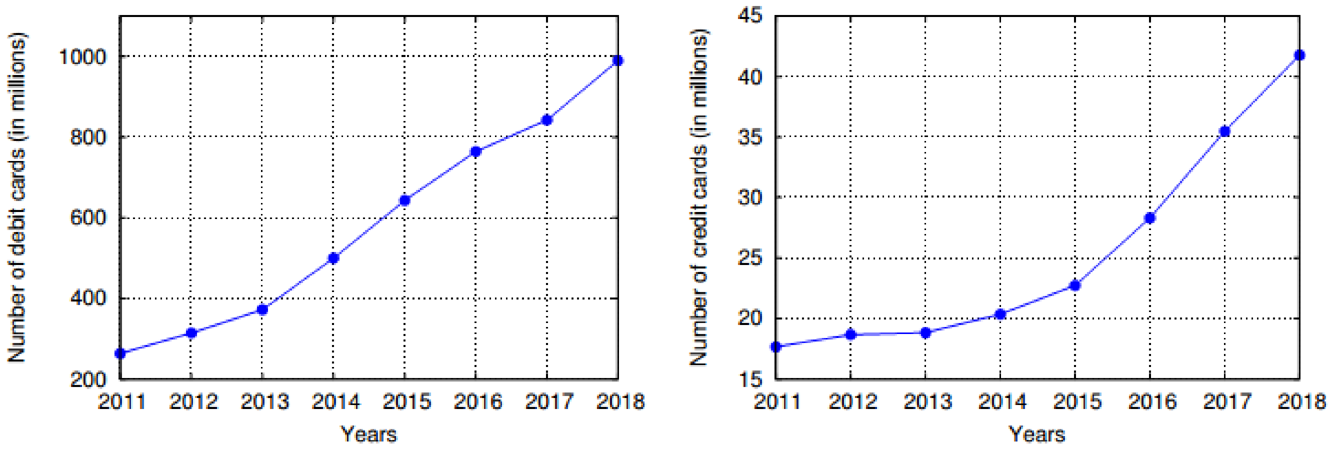
Revised Manuscript Received on October 15, 2019.

* Correspondence Author

Ashutosh Singh*, Department of Computer Science & Engineering, Institute of Engineering & Technology, Lucknow, India. Email: ashu.verve@gmail.com

Ranjeet Srivastva, Department of Information Technology, Babu Banarasi Das Northern India Institute of Technology, Lucknow, India. Email: ranjeetbbdit@gmail.com

Yogendra Narain Singh, Department of Computer Science & Engineering, Institute of Engineering & Technology, Lucknow, India. Email: singhyn@gmail.com



(a) Debit cards

(b) Credit cards

Fig. 2. Payment cards issued from 2011 to 2018 in India.

have grown from $2.1 trillion to $2.56 trillion. In particular, the Asia-Pacific region has generated $102.50 billion payment card transactions that are accounted to 34.68% of worldwide transactions in 2017 [41]. The projected transactions of the card users of this region would reach to 54.03% of worldwide transactions by the year 2027. The US alone has generated $95.11 billion payment card transactions accounting to 32.18% of the total transactions in 2017. Whereas, in Europe and Latin America the total transactions accounted to 65.70 billion and 20.24 billion respectively, shared 22.23 % and 6.19% of worldwide transactions.

In India, government launched a campaign of digital India with an objective to transform the whole country into digitally empowered society. Under this campaign, government has taken several steps of connecting rural areas with high speed internet networks and improving digital literacy. In India, an exponential growth in number of payment card users has been reported from 2011 to 2018 [6]. There were 263 million debit cards and 17 million credit cards active in 2011. The number of debit and credit card users is increased to 989 million and 41.7 million, respectively in 2018 as shown in Fig. 2.

A rapid surge in the digital transactions using credit and debit cards is one of the effects of demonetization policy of government of India. The number of credit card and debit card transactions have grown to 47% and 100%, respectively during twelve months by the end of May 2017 are shown in Fig. 3 [6].

The payment card users increased exponentially, but they are susceptible to Cyber threats and digital frauds. According to a report of Aite group LLC 2010, the card fraud costs the US card payment industry about $8.6 billion per year [1]. The payment threats are closely related to identity theft. The identity theft can be defined as someone using other's identity and the personal information without his/her concern. The identity theft best explains that someone misuses other's personal information such as credit or debit card number and CVV illegally for making illicit payments. The card frauds may be in the form of stolen wallets, skimming, shoulder surfing, keystroke logging.

The frauds discussed above are the serious threats to online payment system. In order to overcome these frauds, an extra level of security can be added to the existing system. This can be done with the integration of user's authentication process using biometrics. Biometrics is a technology to recognize an individual based on his/her unique physical or behavioral characteristics. Unlike PIN or password it cannot be stolen, or exposed to a hostile environment.

This paper proposes a payment card security mechanism that incorporates biometric information of card user along with the existing card verification system. The biometric template of an individual is captured at the time of card issuance and thus prepared template database. During card swipe, the user is required to provide the biometric sample to re-authenticate his/her identity to be matched with the corresponding biometric template stored in the database. For example, the Aadhaar system of India that recognizes individuals on his/her biometric bases can be combined with the existing payment card security system to overcome the most probable issue of identity theft of payment card frauds.

The rest of the paper is organised as follows. The detail of payment card frauds along with the countermeasures taken by different authorities is presented in Section 2. In order to mitigate payment card frauds, an approach that integrates existing payment card security system with biometric recognition of the card user is proposed in Section 3. Section 4 evaluates the performance of the proposed method, in particular statistical analysis to prevent payment card frauds and cost analysis while integrating biometric recognition system are also discussed in this section. Finally, discussion and conclusions are drawn in Section 5.

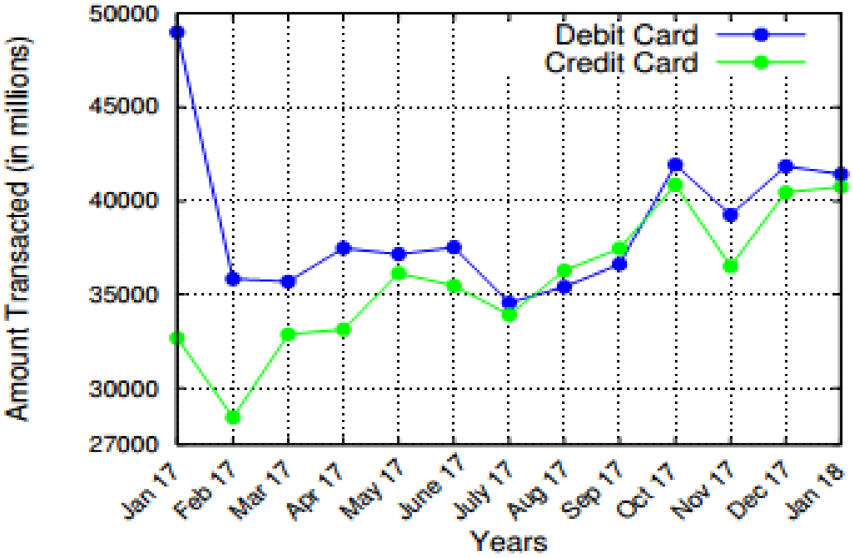


Fig. 3. Number of transactions through debit and credit cards in India.

II. BACKGROUND

There is a whole industry of attackers and thieves who use several ways to commit payment card frauds. The payment card frauds can be classified as follows:

A. Payment Cards Frauds

Stolen wallets: Usually, people carry their cards and other identity information in their wallet. The stolen wallet may result in payment card frauds as well as identity frauds.

Counterfeit cards: A counterfeit card can be prepared by engrossing by encoding genuine details of any individual's card. The counterfeit card is like a genuine card and can be used for withdrawing money, online payment and card swipe. In 2009, the hackers hacked the servers of RBS bank and stole account and PIN information of several payroll accounts. They used the stolen information and created counterfeit cards, thus withdrawn $9.4 million from 2100 ATMs around the world [39]. In 2016, an accused acquired 167 credit cards from several banks and withdrawn 6.3 million India rupees in India [29].

ATM frauds: One of the Indian government undertaking banks, State Bank of India (SBI) has reported fraudulent withdrawals of 3.9 million Indian rupees till Nov 4, 2016 by its 73 cardholders [44]. ATM frauds are one of the most common types of frauds committed daily. It includes manipulating the ATM machine by attaching a device on the number plate that records the number you pressed. A device can also be placed above magnetic strip reader which can collect information about the card and prepares a counterfeit card. A criminal can also force you to withdraw money from the ATM on a gunpoint.

Shoulder surfing: It is one of the most basic techniques adapted by the criminals worldwide to commit card frauds. The criminal can stand next to the victim and peep over to see whatever the victim is pressing, and then they may pick pocket the victim and withdraw the money afterwards [27].

Online transactions: The emergence of giants like Flipkart and Amazon, the online transactions have increased exponentially. It covers around 80% of the total market share. With the increase in the number of online transactions the frauds also increased. As people are becoming dependent on online payment for their commodities they are making purchases through hostile servers, public machines and open wifi's hence making the transactions vulnerable to masquerade and replay attacks. The Reserve Bank of India (RBI) re-ported 10,220 cases of payment card and net banking frauds alone in December 2017 [30].

Keystroke logging: Beware if one is using a public system or wifi for entering your personal details. Softwares like Goldeneye, keylogger may be installed on those systems, which can record whatever keys you are pressing and prepare a log, which can be viewed later. Anything you type like card number or CVV are recorded, and therefore your information is left no more personal. In New York three people were pleaded guilty when they installed keylogger trojan on victim's computer and stole his credentials to access the account [12].

Inside job: The employees of banks or any other financial institutions hold a lot of information about their customers. Many a times these employees sell customer's personal information such as phone numbers and email addresses to companies who want to reach them. These employees also have details about your card number all they need is the CVV to perform any transaction on your behalf, hence recommended not to tell anyone the CVV of your card. In Manila a senior citizen lost

159,000 Peso via unauthorized online fund transfer despite never using his account for the fund transfer [22].

Skimming: Skimming is the process of copying the data stored in the magnetic strip or in a sim of the payment card and uses it to perform illegal transactions. Skimming is mostly done at point of sale such as shop-ping, gas stations and ATM machines. An employee of a shop may use a copying machine, attaches to the swiping device of the ATM and record the data stored in magnetic strip. In 2015, three Romanian nationals were arrested in India when it was found that 9 million Indian rupees were skimmed with a skimmer installed at a Bandra based ATM and over 300 persons had used that ATM during the installation period [3].

B. Payment Card Security Mechanisms

The card service provider ensures a secure payment channel between bank and the point of sale. Although banks have their own security mechanism along with payment card processing security to protect the card user's transactions from different threats. The security measures provided by different authorities are given as follows [33]:

1) Bank - Card Issuer:

- Multi-factor verification of genuine users using PIN or challenging questions is provided as a security measures.
- Multi possession verification is needed whenever a new device is used by the user.
- On detection of some unusual activity the card issuer can place the account on hold or the card can be blocked until verified by the user.

2) Card Companies - Visa or Mastercard:

- The new chip technology replaces the magnetic strip. The chip generates a unique code for every new transaction making it difficult to counterfeit.
- Zero liability makes the user not liable for any trans-action made by someone else using his/her credit card as long as the prompt response is made for any loss or theft to the card company.
- Secure code provides an additional security provided by card issuers that helps their users from fraudulent attacks. A secret code (usually SMS) is sent to the user to re-authenticate his/her identity.

3) Legal Bodies - Government:

- Enacting protection laws for customers related to payment fraud.
- Regular assessment and examinations are done to card issuers.
- Issuing guidelines, and regulations for the protection of card holder and monitoring for and fraudulent activity.

4) Merchants - Point of sale:

- The slip is generated at the time of withdrawal from ATM contains the truncated account number that never reveals user's account number .
- The computer system never stores the original account number associated with card number, instead it gener-ates a random substitute for every PAN. It can mapped to the original data through tokenisation.
- While making payment, any other information in addition to the card number can be used to authenticate the payment such as PIN or ZIP code etc.
- Third party such as PayPal [10], CCAvenue [32] provide a medium between the merchant and the card holder who are unknown to each other, but both are trusted on the third party.

5) Users - Card Owner:

- Never use sensitive data on public machines.
- Passwords and PIN are changed regularly.
- Report of any unusual activity related to their account.
- Never disclose personal information to any one on call or in person.

6) Payment Gateways - PayPal or CCAvenue:

- Once the card details is entered it is encrypted by the payment gateway using public keys. It can only be decrypted using gateways private key, hence protecting it from any type of information leakage among them.
- Secure socket layer is used to establish an encrypted link between the browser and the web-server during online transaction. The SSL certificates also act as a certificate of authenticity to the visiting customers as well as protect the card details of the customer.

The discussed security mechanism provides a defense against card frauds such as card cloning and skimming but still there are loopholes that need to address and making the system robust from fraudulent attacks. The ATM frauds and offline card usage cannot be stopped if the card is stolen and PIN is compromised.

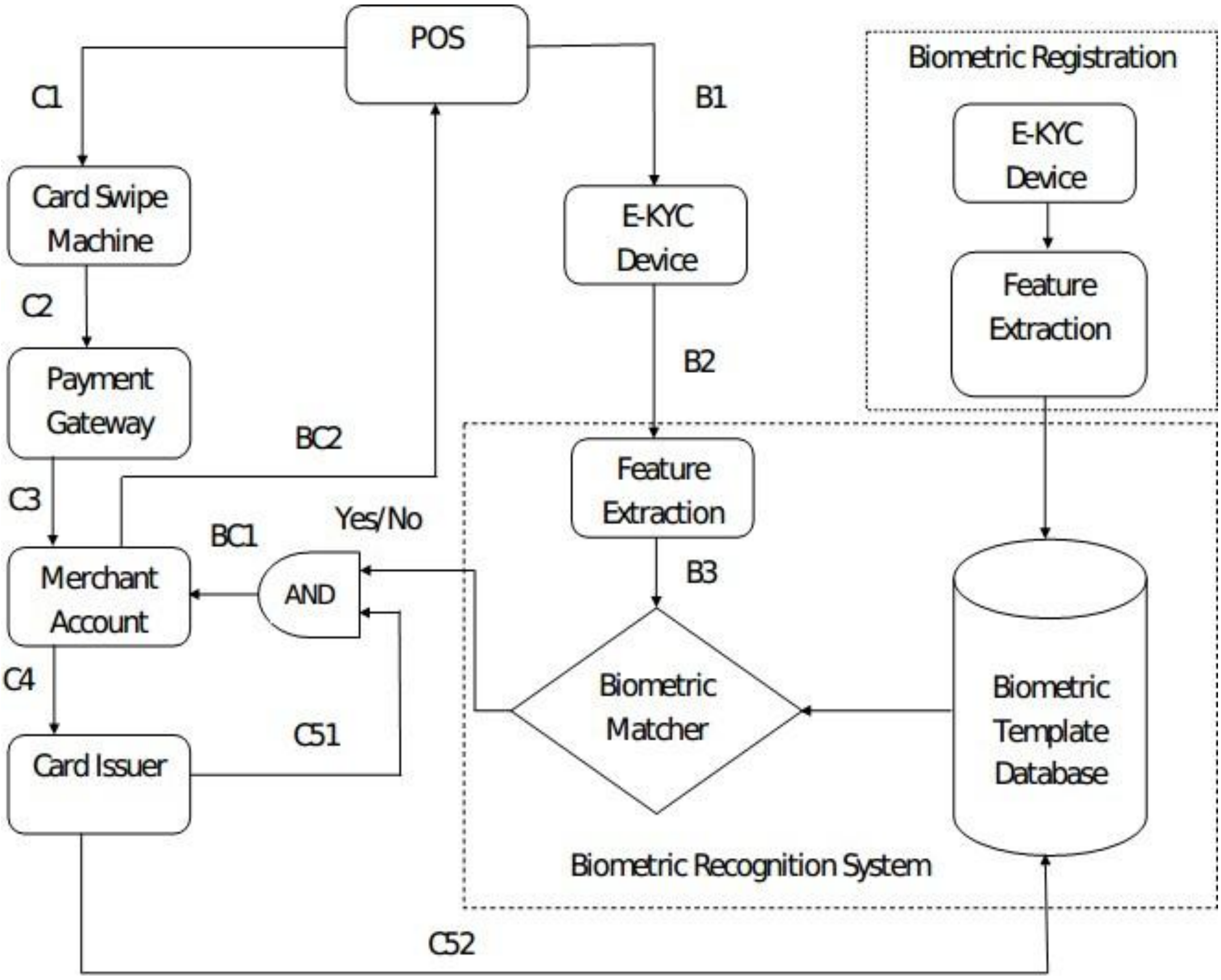


Fig. 4. Schematic of proposed payment card security system using biometrics.

At the time of payment at POS, the only security provided is through PIN, which is easily exploitable by shoulder surfing and skimming.

III. PROPOSED METHOD

The payment card frauds committed either stolen or counterfeited can make them easy for the fraudulent to impersonate and perform illegal transactions. In order to prevent the payment card frauds, this paper proposes a method that works with the existing payment card security system. The method includes biometric recognition system that ensures identity verification of the card user at the time of its application. The biometric modalities such as face, fingerprint or iris need to be acquired from the users as per the availability of the recognition system at the time of the card issuance. Thus, the biometric templates of the card users are prepared and stored in gallery database. The biometric genuinity of the claimant would be established if the query biometric template matches with the corresponding template stored in the gallery. The biometric recognition establishes the authenticity of the card user and thus supplements the payment card security system. A schematic of the proposed system is shown in Fig. 4.

At the point of sale (POS) where a retail transaction is to be completed, the user presents the payment card information (step C1) along with his/her biometric information (step B1). The method assumes that the authentication and verification of the user through the presented payment card data and his/her biometric data, respectively are done in parallel. The swipe machine captures the card number and the associated information from the user that are being sent through a payment gateway for authentication (step C2). These details along with the merchant account number are passed to card issuer (step C3 and C4). The card issuer validates the identity of the card user. The validation result is passed to one input of AND gate (step C51) that waits for the result of biometric verification of the user to its other input (step C52).

Further, at the POS the biometric of the user is acquired for his/her authenticity verification (step B1). The acquired biometric is processed and presented to the matcher that measures the acceptable closeness with its counterpart stored in the gallery database (step B2 and B3). The decision of biometric recognition system such as the ’true’ (genuine) or ’false’ (imposter) is sent to the input of AND gate i.e. result of step C52. The AND gate returns ’true’ if and only if both of its input are ’true’ i.e., the presented payment card details are correct and corresponding biometric is found to be from a genuine user. Finally, it accepts the request of the user to complete the transaction (step BC1 and BC2), otherwise declines.One of the variants of the proposed system is presented as an example of integrating the

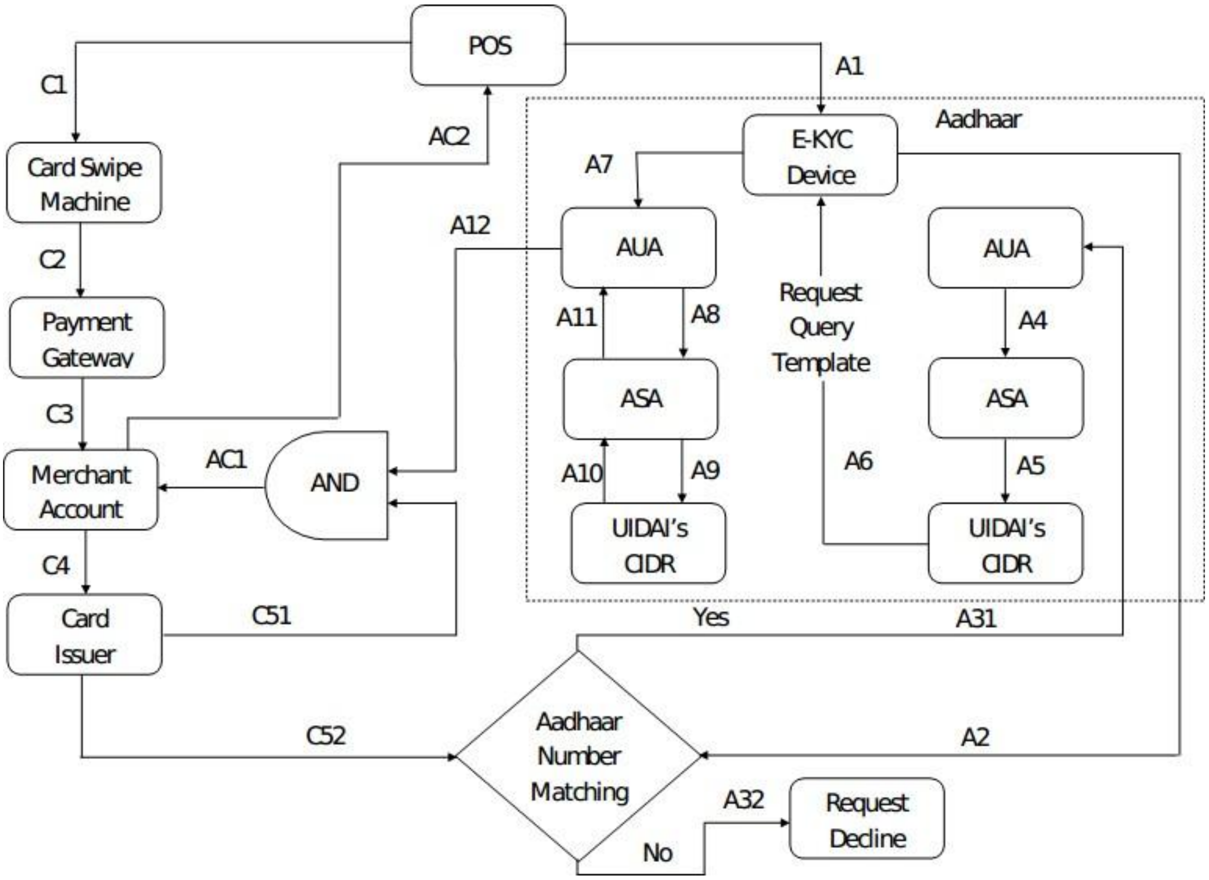


Fig. 5. Schematic of a payment card security system with integration of Aadhaar system.

payment card security system with the Aadhaar system of India. The Aadhaar is world's largest identity project which aims to collect demographical and biometric data of its citizen for authentication mainly for their benefit from government schemes. The UIDAI, a government agency issues an easily verifiable 12 digit random number as a unique identity (UID) called Aadhaar number to all residents of India. Statistically, a total of 1.22 billion citizens (89.7%) are enrolled in Aadhaar till date [9].

A. Payment card security system with Aadhaar

The Aadhaar authentication system provides an online platform for identifying an individual at anytime and anywhere. The Aadhaar authentication service can be available to any requesting agency (public/private) that desires to authenticate the identity of their clients, associates or employees before any type of access is provided to them. There are five actors involved in Aadhaar authentication process:

1. The user that holds the Aadhaar number issued by UIDAI.
2. The authentication device (E-KYC) that collects the identity information of the Aadhaar card user is connected to UIDAI system [4].
3. The central identities data repository (CIDR) stores and manages data of all registered users of Aadhaar [16].
4. The authentication user agency (AUA) is an entity for providing Aadhaar enabled services to its user through authentication service agency (ASA) [35].
5. The ASA works as a bridge between CIDR and AUA. It transmits authentication requests to the CIDR on behalf of AUA [5].

The schematic of payment card security system with an integration of Aadhaar system is shown in Fig. 5. At the POS, user swipes the card and enters the payment card number (step C1) and his/her Aadhaar card number (step A1). It is assumed that the authentication of the user providing the payment card detail and his/her verification using Aadhaar data are done parallely. The user presents the Aadhaar number that is being verified with the Aadhaar number linked his/her bank account (step A2 and C52). Here, Aadhaar is mandatory information provided by the customer to the bank at the time of the card issuance. The request for Aadhaar number matching i.e. its result 'yes' is sent to the AUA (step A31), otherwise 'no' the request is aborted (step A32). Then the AUA requests for the user verification from the repository CIDR. Since, AUA doesn't have direct access to the data repository; therefore the request to the repository is forwarded to the CIDR via ASA (step A4 and A5).
The CIDR on receiving the request, searches its counterpart stored in the database. After a correct match, CIDR prompts the merchant through E-KYC device for biometric data of the claimant (step A6). The acquired biometric data is routed back to CIDR for 1:1 verification through AUA and ASA, respectively (steps A7 A9). The result of CIDR is sent to one of the input of AND gate through ASA and AUA (steps A10 A12).

The other input of the AND gate holds the validation result of the card user presented at POS and processed by the merchant as follows:

The card number and other information captured through swipe machine are sent for authentication through a payment gateway (steps C1 and C2). These details along with merchant's account number are passed to card issuer that validates the customer's card (steps C3 and C4). The result of card validation is routed to one of the input of AND gate (step C51).

Finally, if the presented biometric data and payment card details are both verified, then the processing request is granted (steps AC1 and AC2). Otherwise, if anyone of the provided information such as payment card detail or biometrics does not match with their bank or the Aadhaar system, the result at AC1 is false. Thus results in a decline of processing the request (step AC2).

IV. Performance evaluation

This section presents the performance evaluation of the proposed payment card security system using biometrics. Statistically, security analysis of the method is done considering perfectness of the used biometrics. Subsequently, cost analysis of the method is also presented.

A. Security Analysis

The present payment card security system validates the authenticity of the card user primarily through a PIN. The PIN is usually 4-6 digits random number [11]. The PIN may be user defined but controlled by card issuing authority. Under prevailing security mechanism of payment cards, the probability of guessing the user's PIN (4-digit) by an intruder is $3/10^4$, providing the number of chances to enter the correct PIN is three. More formally, if a PIN consists of n_1 digits and the number of allowed attempts (guesses) to enter the PIN are k_1, then the probability of guessing the correct PIN (PGuess), by an intruder is,

$$PGuess = \frac{k1}{10^{n_1}} \qquad (1)$$

The intruder attempts to guess the correct PIN of n_1-digits out of 10^{n_1} possibilities. Although the probability of guessing the PIN looks moderate, the probability of guessing the correct PIN is 1, if the intruder exactly knows the combination of n_1-digits.

The proposed method integrates present payment card security system with biometric recognition of the user. The system like Aadhaar may be used for biometric recognition of an individual that supplements the security system of payment cards. The validation of card user using biometric along to presented card information overcomes the issues related to PIN security. The method uses Aadhaar number and performs biometric verification of the cardholder in real time.

The integration of Aadhaar with payment card security system using PIN makes the system robust against card frauds. More formally, the probability of breaching the security of payment card (P_{Breach}) can be computed as,

$$P_{Breach} = P_{Guess\ PIN} \times P_{Gue\,ss_{UID}} \times FAR \qquad (2)$$

Where$P_{Guess\ UID}$, is the probability of guessing the Aadhaar number and FAR is the false acceptance rate of the biometric in the Aadhaar system. Since, UID contains 12 decimal digits, therefore $P_{Gue\,ss_{UID}}$ is $3/10^{12}$, assuming the number of chances to enter the correct UID is 3. In general, let security identification number be of size n_2 and the number of allowed chances to enter it correctly is k_2, then possibility of guessing the security identification number $P_{Guess\ S/N}$ can be defined as,

$$P_{Guess\ S/N} = \frac{k_2}{10^{n\,2}} \qquad (3)$$

The FAR of a biometric recognition system computes the likelihood of falsely accepted users over a given population. The proposed method can work with any of the biometric modalities such as face, fingerprint or iris as used in the Aadhaar system.

In Eq. (2), the probability of breaching payment card security (P_{Breach}) is extremely low. For example, if we use the face biometrics for the verification of an individual along with the PIN, then

$$P_{Breach} = \frac{k1}{10^{n\,1}} \times \frac{k2}{10^{n\,2}} \times \left(\frac{2}{10^2}\ to \frac{4}{10^2}\right) \qquad (4)$$

The FAR of the face recognition system are reported to 2% to 4% invariably from constrained to unconstrained environments, respectively [20].

For fingerprint biometrics P_{Breach} can be found as,

$$P_{Breach} = \frac{k1}{10^{n\,1}} \times \frac{k2}{10^{n\,2}} \times \frac{1}{10^2} \qquad (5)$$

Where, FAR for fingerprint recognition system is reported to 1% [20]. Similarly, P_{Breach} for the iris recognition system can be computed as,

$$P_{Breach} = \frac{k1}{10^{n\,1}} \times \frac{k2}{10^{n\,2}} \times \frac{0.01}{10^2} \qquad (6)$$

Where, F AR for an iris recognition system is reported to 0.01% [20].

Let us assume that the number of chances for guessing the PIN k_1 and the UID k_2 number are three, number of digits used as PIN (n_1) is four and the size of UID number (n_2) is 12. Then, Eqs. (4) - (6) can be rewritten as,

$$P_{Breach_{Face}} = \frac{k1}{10^4} \times \frac{k2}{10^{12}} \times \frac{4}{10^2} = 3.6 \times 10^{-17} \qquad (7)$$

$$P_{Breac\,h_{Finger}} = \frac{k1}{10^4} \times \frac{k2}{10^{12}} \times \frac{1}{10^2} = 9 \times 10^{-18} \qquad (8)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$$P_{Breach_{Iris}} = \frac{k1}{10^4} \times \frac{k2}{10^{12}} \times \frac{0.01}{10^2} = 9\times 10^{-20} \qquad (9)$$

From Eq. (7) - Eq. (9), it can be observed that the values of P_{Breach} are found to be extremely low for all biometrics whereas lowest for iris biometric.

The Aadhaar system leaves three options to its user for his/her biometric recognition using the face, fingerprint or iris. Under accuracy consideration the used biometrics must have lowest FAR. Iris may be one of the best biometrics to supplement user's authentication process in terms of lower FAR. When considering users convenience, fingerprint may be the best biometric to re-authenticate the card user along to payment card security process. Further, payment card security system with biometric verification using face would be another option with lowest FAR to be developed in the future.

B. Cost Analysis

The biometric recognition of the user supplements the payment card security system. For example, when Aadhaar system is integrated with the existing payment card processing system then the cost involves mainly due to total time elapsed in processing the transaction that needs to be analyzed. The Aadhaar system works using 12-digit UID number. At the POS, the user provides the payment card details along with the unique ID. Each digit represents using 4 bits as 0000 to 1001 (from 0 - 9). Thus, six bytes data is sent over network as pay-load. It additionally attaches header that includes checksum, source and destination addresses. The system (E-KYC device) generates the frame that is of small size whereas the data transmission rate is very high e.g., fibre optics channels are used mostly for data transmission. Therefore, frame generation time is considered to be negligible.

The UID data is sent to the bank for matching with the customer's Aadhaar details linked with his/her account. If the match is found then the UID number is sent to the nearest CIDR through a secure channel provided by the ASA. The transmission time for the data to reach the CIDR is negligible due to the distance from the nearest CIDR is found to be the order of a few thousand kilometers whereas data transmits at the speed of 2×10^8 m/sec using optical fiber cable.

Therefore, the total time taken for the data to be generated and be available at the CIDR is considered negligible. The time taken to find the correct data in CIDR among *N* Aadhaar users depends upon the employed search technique and its processing time which is machine dependent i.e.,

i. The number of instructions the technique have I,
ii. Number of cycles used per instruction C, and
iii. The cycle time T.

The processing time T_p, can be defined as the product of above three parameters as,

$$T_p = I \times C \times T \qquad (10)$$

Let the number of comparisons done to find the correct match in CIDR is *k*, where $N = 2^k$. Therefore, the time required to search the claimant's ID to its counterpart in CIDR database can be computed as,

$$Ta = k \times Tp \qquad (11)$$

After a correct match, CIDR requests for the query template from the user. The query template is sent to the CIDR for matching the searched template from the gallery via ASA. Let the time required in biometric matching be T_b then the payment card processing time can be reported as,

$$Tc = Ta + Tb \qquad (12)$$

Let the population covered under Aadhaar be 1.25 billion ($\approx 2^{30}$), then k = 30. Assuming that the searching program contains 20 instructions, computing machine with 3.5 Ghz processing speed and an average of 1 cycle per instruction then the time elapsed in Aadhaar number comparison can be computed using Eq. (10) as 17 nanoseconds. For biometric verification if a template contains 30 biometric features on average and matching each feature requires 20 instructions, the total time for biometric verification would be 17 nanoseconds. Therefore, the overall time taken for the Aadhaar verification is insignificantly low.

V. RESULTS AND CONCLUSION

The proposed formulation for preventing credit card frauds using biometrics verification of the users provides another level of security to the existing chip and PIN system. Biometrics is a technology that works on physiological and behavioral characteristics of a person for his/her recognition. The body parts such as the face, fingerprint, iris, hand geometry and other behavioral characteristics such as voice and signatures are being used for authentication of the individuals. The biometric system using conventional modalities have shown good trade-off between genuine acceptance rate and false acceptance rate whereas their deployment depends upon the cost, speed and applications.

The card-not-present transactions (CNP) are made for payment card transactions where the cardholders do not physically present the card to the merchant for visual examination. The CNP may cause credit card frauds because it is harder for the merchant to verify the identity of the card holder claiming for transactions. The CNP causes more than 50% of all fraud losses of worldwide transactions. The purchase made by payment cards in global and domestic market reached to 34.12 trillion in 2017 whereas the cumulative loss due to payment card frauds was $24.26 billion. By 2022, the total transactions the using payment card is projected to $56.17 trillion whereas the card fraud losses would be $34.66 billion worldwide [42]. The proposed framework for the prevention of payment card frauds may reduce the overall fraud losses to the negligible level. For example, if the cost associated to the Aadhaar system is $1.4 billion by the end of March 2018 and the expected losses are $31.26 billion, then the biometric verification using Aadhaar costs significantly low (~ 4%) in comparison to total losses incurred that year.

The social and ethical factors may affect the selection of an appropriate biometric that emulates the payment card security system. For example, the biometric modality like fingerprint can be used for users verification but environmental factors such as manual laborers and the places of extreme cold may prevent their users from verification process due to lack of clear fingerprints or minutia displacement due to low compliance of friction ridges. The card users may have some reservations to use their iris for verification because they have to keep their eyes open under intense lighting conditions.

This paper has proposed a novel approach to prevent the payment card frauds using biometrics. The integration of biometric verification to the existing payment card security system may ensure the presence of the card holder at the time of its processing and thus, prevents from fraudulent attacks with no possibility to commit stolen card frauds. The proposed system may be robust enough against payment card frauds such as, counterfeit cards, ATM frauds, keystroke logging, skimming and shoulder surfing.

However, the biometric security has their own challenges related to secrecy and privacy of the users but the agencies like UIDAI has ensured that the Aadhaar system follows the standard protocols that can limit these challenges. The wide coverage of UIDAI i.e., over 99% of adult population of India provides an opportunity that Aadhaar system may be integrated with payment card processing system for the prevention of payment card frauds. Therefore, the proposed system may definitely pave the way of a better environment for the cashless society with no concerns of card frauds.

REFERENCES

1. 2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From. [Online Available at] https://www.aitegroup.com/report/2016-global-consumer-card-fraud-where-card-fraud-coming. Accessed on: Feb 6, 2019.
2. A. Bisht, P. Nair, R. Dubey, T. Hajela, "Analysis of the use of plastic money: A boon or a bane", SIMS Journal of Management Research, Vol. 1, 2015.
3. ATM skimming fraud. [Online Available at] http://indianexpress.com/article/cities/mumbai/atm-skimming-fraud-300-people-may-have-lost-money-at-bandra-atm/. Accessed on: Feb 15, 2019.
4. Authentication Devices. [Online Available at] https://uidai.gov.in/authentication/authenticationdevicesdocuments/device s.html. Accessed on: Feb 22, 2019.
5. Authentication Service Agency (ASA). [Online Available at] https://uidai.gov.in/authentication/authenticationpartners/serviceagenc. html. Accessed on: Feb 22, 2019.
6. Bankwise ATM/POS/Card Statistics. [Online Available at] https://rbi.org.in/scripts/atmview.aspx. Accessed on: Feb 5, 2019.
7. Bankwise Volumes in ECS/NEFT/RTGS/Mobile Transactions. [Online Available at] https://rbi.org.in/Scripts/NEFTView.aspx. Accessed on: Feb 5, 2019.
8. Bo Carlsson, "The Digital Economy: what is new and what is not?", Structural Change and Economic Dynamics, Elsevier Vol 15, Issue 3, 2004, pp. 245-264.
9. Budget 2018. [Online Available at] https://economictimes.indiatimes.com/news/economy/policy/budget-2018-go vernment-mulls-aadhaar-like-unique-identity-for-business-says-jaitley/articleshow/62738792.cms. Accessed on: Feb 18, 2019.
10. CCAVenue for payment gateway. [Online Available at] https://www.ccavenue.com/. Accessed on: Feb 3, 2019.
11. Credit card fraud. [Online Available at] https://en. wikipedia.org/wiki/Credit card fraud. Available: Accessed on: March 13, 2019.
12. Defendant pleads guilty in brokerage keylogger case. [Online Available https://www.scmagazine.com/defendant-pleads-guilty-in-brokerage-keylogger -case/article/555976/. Accessed on: Feb 15, 2019.
13. Digital Density Index: Guiding Digital Transformation. [Online Available at] https://www.accenture.com/us-en/insight-digital-density-index-guiding-digital-transformation.html. Accessed on: Feb 24, 2019.
14. Digital economy. [Online Available at] https://www.sciencedaily.com/terms/digital economy.htm. Accessed on: March 02, 2019.
15. Digital economy. [Online Available at] https://en.oxf orddictionaries.com/definition/digital economy. Accessed on: March 02, 2019.
16. Enrolment Agencies. [Online Available at] Online Available at https://uidai.gov.in/enrolment-update/ecosystempartners/enrolment-agencies.html. Accessed on: Feb 22, 2019.
17. Eric B. and Brain K, "Understanding the digital economy: Data, Tools and Research", The MIT Press, 2002
18. FederalCommissionReport,2013,"https://www.ftc.gov/stystem/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf".
19. Flipkart Investigates Online Shopping Fraud Leading To Arrest of 2 Techies. [Online Available at] http://trak.in/tags/business/2015/12/26/flipkart- fraud-arrest-of-2-hyderabad-techies/. Accessed on: Feb 15, 2019.
20. J. G. Daugman, High Confidence Visual Recognition of Persons by a Test of Statistical Independence, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.15, No. 11, pp. 11481161, 1993.
21. Ian Ross, "Exposing Fraud: Skills, Process and Practicalities", Wiley Edition, 2016.
22. Inside job? [Online Available at] http://news.abs-cbn.com/business/09/18/15/inside-job-senior-citizen-loses-p159000-unauthorized-online-transfer. Accessed on: Feb 15, 2019.
23. J. Steel, "Credit card fraud and ID theft statistics". [Online Available at] https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. Accessed on: March 6, 2019.
24. J.Wright, "Optimal card payment systems", European Economic Review, Elsevier, 47(2003), pp. 587-612.
25. L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithms and performance evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20(8), 1988, pp. 777-789.
26. Maes, S, Tuyls, K, Vanschoenwinkel, B, Manderick, B, "Credit card fraud detection using Bayesian and neural networks", Proceedings of the 1st international NAISO congress on neuro fuzzy technologies,Havana, Cuba, 2002.
27. M. Kumar, T. Garfinkel, D. Boneh, T. Winograd, "Reducing Shoulder-surfing by using Gaze-based Password entry", In Proceedings of the 3rd symposium on usable privacy and security, Pennsylvania, USA, 2007, pp. 13-19.
28. M. Ivan., R.B. Kasper., R. Marc. "Pulse-Response: Exploring Human Body Impedance for Biometric Recognition." ACM Transactions on Privacy and Security, Vol. 20, No. 2, Article 6, May 2017.
29. Now, fake PAN, voter cards scam. [Online Available at]. http://www.thehindu.com/news/cities/Hyderabad/now-fake-pan-voter-cards-scam/article7557121. Accessed on: Feb 10, 2019.
30. Over 25,800 online banking fraud cases reported in 2017: Govt. [Online Available at] http://www .livemint.com/Industry/ 5qv8uvgNJFmnXvLcri4boM/ Over-25800-online-banking-fraud-cases-reported-in-2017-Gov.html. Accessed on: Feb 10, 2019.
31. Payment Card Fraud [Online Available at]. https://nilsonreport.com. Accessed on: Feb 5, 2019.
32. Paypal Third party payment. [Online Available at] https://www.paypal.com/us/webapps/mpp/payflow-payment-gateway. Accessed on: Feb 3, 2019.
33. Peace of mind with Mastercard? security [Online Available at]. https://www.mastercard.us/en-us/consumers/get-support/safety-and-security.html. Accessed on: Feb 15, 2019.
34. Predictions About The Future Of Digital Transformation [On-line Available at]. http://www.forbes.com/sites/gilpress/2015/12/06/6-predictions-about-the-future-of-digital-transformation/1d47b8e725b4. Accessed on: Feb 25, 2019.
35. Requesting Entities (AUA& KUA). [Online Available at]. https://uidai.gov.in/authentication/authenticationpartners/useragency. html. Accessed on: Feb 22, 2019.

https://arxiv.org/pdf/1708.05117.pdf. Accessed on: March 14, 2019.

36. S. Patil, "Impact of plastic money on banking trends in India", International Journal of Management research & business Strategies, Vol. 3, No. 1, 2014 pp. 224-236.
37. Symposium on Digital Business in Rural India: Opportunities and Challenges. [Online Available at]. http://digitalindia.gov.in/node/10110. Accessed on: Feb 15, 2019.
38. The Analyzer Hack Probe Widens; $10 Million Allegedly Stolen From U.S. Banks. [Online Available at]. https://www.wired.com/2009/03/the-analyzer -ha/. Accessed on: Feb 6, 2019.
39. The Ferderal Reserve Payments Study - 2017 [Online Available at]. https://www.federalreserve.gov/paymentsystems/2017-December-The-Federal-Rese rve-Payments-Study.htm.
40. The Nilson Report Oct, 2018. [Online Available at] https://nilsonreport.com/publication newsletter archiveissue.php?issue=1140 Accessed on: Jan 20, 2019.
41. The Nilson Report Oct, 2018. [Online Available at] https://nilsonreport.com/publication newsletter archive issue.php?issue=1144 Accessed on: Feb 12, 2019.
42. Wayman J., Jain A., Maltoni D., Maio D. (2005) "An Introduction to Biometric Authentication Systems". In: Wayman J., Jain A., Maltoni D., Maio D. (eds) Biometric Systems. Springer, London.
43. http://www.deccanchronicle.com/business/in-other-ne ws/221116/data-breach-73-sbi-cardholders-reported-fraud-withdraw.

AUTHORS PROFILE

Ashutosh Singh recieved the B.Tech and M.Tech degree in Computer Science & Engineering from Uttar Pradesh Technical University, Uttar Pradesh, Lucknow. He is currently working as research scholar in Computer Science & Engineering at Institute of Engineering & Technology, Lucknow, India. His research interests include biometric template security, pattern classification and machine learning. He has published two research papers in International Journals/ Conferences of repute.

Ranjeet Srivastva recieved the B.Tech degree in Information Technology from Uttar Pradesh Technical University, Uttar Pradesh, Lucknow, India in 2008 and M.Tech degree from Guru Govind Singh Indraprastha university, Delhi, India in 2013. Since then he is working as Assistant Professor in the department of Information Technology, Babu Banarasi Das Northern India Institute of Technology, Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India. He is pursuing Ph.D in Computer Science & Engineering from Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India. His research interests include pattern analysis & classification, biometric recognition and signal processing. He has published seven research papers in International Journals/ Conferences of repute.

Yogendra Narain Singh is working as Professor in the department of Computer Science & Engineering at Institute of Engineering & Technology, Dr. APJ Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India. He received the M. Tech. degree in Computer Science & Engineering at Indian Institute of Technology Kanpur, India and Ph. D. degree at Indian Institute of Technology (BHU) Varanasi India. He has authored two books. He has to his credit over forty research articles published in International Journals/ Conferences of repute. Dr. Singh is interested in the areas of pattern recognition, machine learning methods & algorithms, computer vision, medical image computing and biometrics. His research aim is to explore the knowledge of mathematics, artificial intelligence, cognitive science, and biological sciences to provide the solutions to the problems related to biometric recognition, machine vision, intelligent medical computation and human computer interaction. He is pioneer in biometric research in particular, he developed the state-of-the-art biometric system that recognizes individuals using a novel biometric electrocardiogram (ECG). He is one of the researchers whose paper is selected the best biometrics-related papers across the Elsevier journals.