www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-5, October 2018
Review Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

Security for Digital Payments: An Update

Shubham[1*], Deepak Chahal[2], Latika Kharb[3]

[1]MCA, JIMS, Rohini,Sector-05, New Delhi, India
[2,3] IT, JIMS, Rohini,Sector-05, New Delhi, India

[*]*Corresponding Author: latika.kharb@jimsindia.org*

Received: 03/Oct/2018, Accepted: 17/Oct/2018, Published: 31/Oct/2018

***Abstract*—** A cashless economy is secure and it's clean too. Electronic banking, also known as electronic funds transfer, is simply the use of electronic means to transfer funds directly from one account to another, rather than by check or cash.The financial security over the digital payment channel is important for pushing the cashless economy idea.There have been a lot of development of many security protocols to ensure the security in online transactions. However, there are some loop holes in the present e-commerce payment systems. The article focuses on all the aspects of the Security system in Digital Payments in India.With the continuous growth of Internet, the trend of on-line business is extremely high. The aim of this paper is to discuss what are the challenges in digital payment system, how to ensure that your digital data is secure, how to provide security of data to all.

***Keywords*—** Demonetization, Cashless Transaction, Parallel Economy, Money Laundering, Electronic Funds Transfer

I. INTRODUCTION

The word Cashless means "the use of electronic methods rather than the use of cash." Without the internet, we cannot the imagine usage of Digital Payment. The history of internet was started around in 1969 with ARPANET. In 1990 when internet was going up, we did a little bit of digital payments and in 1994 a institute called Stanford Federal Credit Union was established that gave the facility of banking services to the customers. Initially, the online payments were not much secure and user friendly. In 1994 Amazon Co. was established and Pizza hut started the online food ordering for its customers. In 1998 Paypal also started a firm whose aim is to provide a wireless transaction to customers. After this, Paypal kept on developing new innovations like sending payments using the Email. You have a leadership role to play in taking India towards an increasingly digital economy-Narendra Modi[1].

Almost all of the digital payment system are user-friendly in nature which means you don't have the need to install some additional software or buy special equipment for making a payment because all payments are totally based upon the web based or mobile based applications.

Recently, Research and Markets has announced the addition of the "Digital Payment Systems Market in India - Drivers, Opportunities, Trends, and Forecasts to 2022" [2] that **t**he Digital Payment Systems Market in India market will witness a CAGR of 58.90% during the forecast period FY2017-FY2023. In this research, it is found that more than 80% of urban population and about 70% of retail sector got shifted towards digital payment and it also expected to that digital payment industry will reach $700 billion by 2022 in terms of value of transactions. This is a very big value and it is good for Indian economy and for its development.

A. Key Points for the acceptance of Digital Payment

- According to Live Mint study on Mobile Internet users in India on 24th March 2017, India has become the 3rd largest internet user in the world: out of which 50 percent of them are only mobile internet users. This seems to be a significant large data but still it represents only 19 % of India's total population using internet. This number may increase due to the digital payment impact.
- The Government of India also takes action and initiative to increase the digital payment. According to KPMG, NASSCOM, June 2016, The Indian FinTech software market is forecasted to touch USD2.4 billion in the year 2020 from the current USD1.2 billion.

B. Issues and challenges in Digital Payment System

- *Lack of usability:* -Electronic payment system requires large amount of personal data or information from end users to make transactions like credit card payments through website requires large amount of information to make payment.
- *Inadequate laws:* -The laws related to digital payment are varying from traditional laws or it may be unclear. E-wallets are comes under non

bankingfinancial companies (NBFC) so the traditional banking laws are not applicable.

- *Data protection and security:* - Security compliances for "FinTech"companies are come underSection 43 A of the Information Technology Act (which covers data protection). Although digital banking is considered relatively safe but in last few months this arises question in Indian Banking Security System because approximately 3.2 million debit cards were hacked. So this is one of main issue for India in the development of cashless economy.
- *Acceptance of e-Cash:* -In many countries e-Cash is not accepted because it is necessary that the retailers or any other commercial institute accept it as a payment method.
- *Lack of awareness:* -Making payment online needs some knowledge to do it. This problem is more in rural areas where people are still uneducated or less educated so they always prefer their traditional way to make payment rather than go to digital one.
- *Lack of Grievance Redressal Mechanism:*-Lack of grievance redressal is also one of the main issue while doing payment digitally because there are not any proper address regarding grievance.For example, if the recipients face any delay, or if there are discrepancies in the payment amounts, who is to be held responsible? Should the consumer go to the banks or to the relevant government department initiating the cash transfer?

II. SECURITY CONCERN

For promoting digital payment system or go cashless in country like India Security is one of the main issue for individual as a whole. From the last few years we have noticed many cyber security attacks in all over the world and in almost all sectors like telecom, banking, e-commerce etc with make cyber security as biggest challenges for world. In India, 3.2 million customers' card data was hacked. State Bank of India, India's largest bank, on October 19th 2016, stated that it had blocked close to six lakh debit cards following a malware-related security breach in a non-SBI ATM network. Due to the massive data breach, Indian banks have decided to either replace or request users to change the security codes. However, in certain cases banks have decided blocked the cards or issue fresh ones.

Malware is malicious software program that include viruses, worms, Trojans andany other threads that damages computer systems at ATMs or bank servers, and allows hackers to steal confidential credentials of users and whenever user swiped their cards at an allegedly compromised ATM it is possible that data on card along with security PIN to be transmitted to hackers and then they use it illegally.

III. PROPOSED SOLUTION

Before To overcome the security problem of digital payment and to encourage cashless economy Government along with RBI adopts some important technologies and include them in Online Payment Policy, which secure digital payment more sufficiently[3]. For example

A. Encryption:

Encryption is basically a process of converting confidential data and information in a form of code, which prevent from unauthorized access. Whenever we make online payment the first question arises in our mind that 'is online payment safe and by how much?'. However most online payment accepters use an encryption mechanism to secure user personal and payment information. There are various types of encryption technique are in use which prevent unauthorized access or stealing of user payment data like RSA(Rivest-Shamir-Adleman), Triple DES(Data Encryption Standard), Blowfish encryption, AES(Advanced Encryption Standard), etc.

B. Digital Signature:

The parties involved in online payments, transactions should use digital signatures in order to ensure authentication of transactions.

C. Firewalls:

Firewalls simply means secure a system or network from unauthorized access. Firewalls can be used to filter the incoming or outgoing traffics based on a set of security rules called as Firewall Policies.

Firewalls policies can be of three types:

- *Acceptance:*Permits the user after passing through firewall.
- *Dropped:* Not allowed, no indication of failure.
- *Rejected:* Not allowed through, informs the sources that the packet was rejected.

IV. ADVANCED SECURITY OPTION

A. Secure Sockets Layer (SSL) protocol:

Secure Sockets Layer is developed by Netscape Communications Corporation in 1994 to secure online transactions. SecureSockets Layer (SSL) is a standard security technology for establishing an encrypted links between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client (e.g., Outlook). Generally, data sent between web server and browser is a plaintext[4]. A plaintext is a normal text that is sends to receiving system after encrypted into ciphertext by applying encryption algorithm. At receiving unit the receiver decrypt this ciphertext using decrypted algorithm so they read the message or information.

However SSL provide more secure way to transfer sensitive information like credit card details, user login credentials, bank account details etc. SSL is a moreover, a security protocols, a protocols that defines how the algorithm work behind it. SSL provide a two way mechanism for the encryption of both the link as well as the data which is being transmitted. It provides a well environment where all browsers can interact with a secured web server, but there is a condition for their interaction, that is both the web server and the browser need SSL Certificate to established connection. SSL secure millions of confidential and sensitive information of user especially when they do online transaction or in other words called digital payment[5].

B. Working of SSL

- When a browser attempts to create a connection with a SSL secured website then a SSL connection is established between browser and web server using a process called "SSL Handshaking". This process is hidden from the user and it happens instantaneously.
- For creating a SSL connection three keys are used: Public key, Private key and Session key, so the plaintext can only be encrypted with the public key and only be decrypted with the private key and vice-verse.

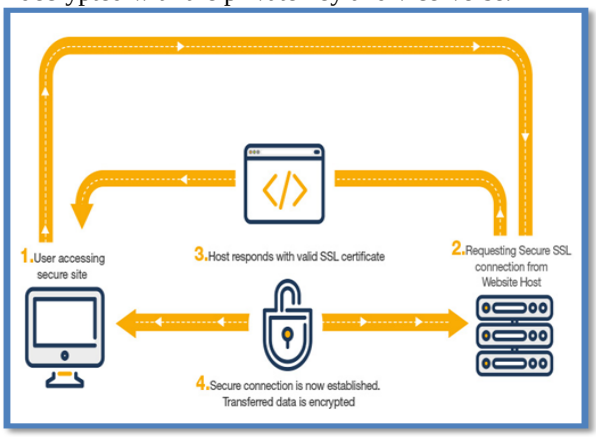

Fig 1- Secure Socket Layer (SSL)

- Encryption and decryption of plaintext to ciphertext and vice versa using public key and private key consume lot of processing power, so they are only used during the SSL Handshaking to create a symmetric Session key. After the successfully establishment of SSL Handshaking connection, this session key isused to encrypt all the transmitted data.
- Browser requests the web server or website which is secured with SSL protocols to identify it and create a SSL connection.
- Server sends a copy of its SSL certificate along with server's public key to browser to make connection.
- Browser checks the certificate root against all the necessary trusted protocols and if the browser trusts the certificate then it made a connection, encrypt, and sends back a session key by using server's public key.
- Server decrypt the session key with the help of available private key and sends back an acknowledgement with encrypted session key to start encrypted session.

After successfully started session, Server and Browser are now able to encrypt all data with the session key, now there is no need of public key and private key.

B. Transport Layer Security(TSL) Protocol:

After the success of SSL protocol, the Internet Engineering Task Force(IETF) decided to develop a standard protocol in the name of SSL 3.0 which later becomes as TSL protocol. It has same functionality as SSL but with slighter more advanced. It provides more secure internet transaction between web and browser. Other than that it also used in other application protocols, such as File Transfer Protocol (FTP), Lightweight Directory Access Protocol (LDAP), and Simple Mail Transfer Protocol (SMTP). Transport layer protocol provide more secure user authentication, data encryption, server authentication, data integrity[6].

- **Key Point related to TSL**
  - TSL uses Hashingfor Message Authentication Code (HMAC) algorithm which overrides the SSL Message Authentication Code (MAC) algorithm.
  - HMAC produces more secure hashes than the MAC algorithm.
    - It includes many new alert messages.
    - In TSL, instead of including all certificates we can work by using intermediate authority only.
    - TLS specifies padding block values that are used with block cipher algorithms.

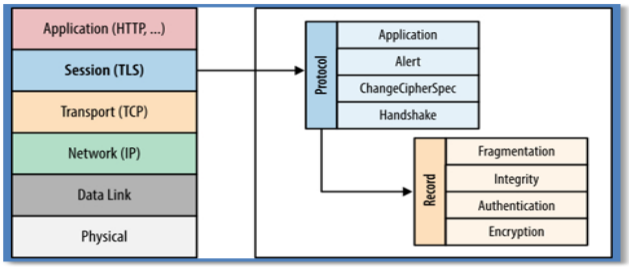

Fig 2- Transport Layer Security (TSL)

- **Benefits of TSL**
  - **Interoperability:** TSL works on almost type of operating system like Microsoft Window, UNIX, Sun Solaris etc. It also supported for every browser such as Microsoft Internet Explorer, Netscape Navigator.

- **Algorithm Flexibility:** It provides option for like user authentication, encryption algorithm, and hashing algorithm for secure connection.
- **Ease of deployment:** It can be easily deployed on the system by select the checkbox, if the server has server certificate installed[7].
- **Ease of use:** TSL is used beneath the application layer so it is completely hidden from the client and so protected from attackers.

C. Secure Electronic Transaction (SET) Protocol:

Secure Electronic Transaction protocol is a method for secure financial transaction on the Internet. It has capabilities to operate in both condition real times as well as on the Internet. It is supported by Microsoft, Netscape, Visa, MasterCard and many others.

- *Key points:*
- With SET, an *electronic wallet* or also called *digital certificate* is giver to user and when user made a connection it is verified using the combination of digital certificates and digital signature in a way that ensure privacy and confidentiality.
- SET uses the Microsoft's Secure Transaction Technology (STT), Terisa System's Secure Hypertext Transfer Protocol (S-HTTP) and Netscape Secure Sockets Layer protocol (SSL).
- It does not uses the all the concept of public key infrastructure (PKI).
- SET must follow certain criteria for secure transaction such as [8]:
- **Confidentiality:**Confidentiality simply means other cannot monitor exchanges.
- **Integrity:** Integrity means identical, what message received is same as what user sent.
- **Authenticity:** It means you must be self-possessedbefore making any type of transaction with others.
- **Non-Reputability:**You must assure that receiving parties cannot deny from the transaction.

The SET protocol has three principle features:

- All confidential information and credential of user which is sent between the three parties must be encrypted.
- All the three parties must authenticate themselves with digital certificates.
- Customer's card number is never seen by merchant in plaintext.

V. CONCLUSION

However, the initiative taken by the Government of India to scrape the old currency is shock to the economists but it's very helpful in creating awareness about digital payment among the people and due to this more people shifting towards cashless economy and adopting digital cash as their first choice and participate in the Government vision to make India Cashless and Smart. But the security issue must be taken seriously by the Government and RBI as well as Cyber Security of India and a secured system must be implemented in a timely manner.

REFERENCES

[1] Jain, M., & Nagpal, A. (2017). From Cash to Cashless Economy: Catalytic Agent for Financial Inclusion? MUDRA : Journal of Finance and Accounting,4(01).

[2] Tiwari, R. (2017). Impact of Demonetization on Indian Economy: A Survey. IOSR Journal of Economics and Finance, 08(02), 01-05.

[3] Panja, B., Fattaleh, D., Mercado, M., Robinson, A., & Meharia, P. (2013). Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. 2013 International Conference on Collaboration Technologies and Systems.

[4] Day, D. (2014). Seizing, imaging, and analyzing digital evidence. *Cyber Crime and Cyber Terrorism Investigators Handbook*, 71-89.

[5] Fink, D. (n.d.). Identifying and Managing New Forms of Commerce Risk and Security. IT Solutions Series: E-Commerce Security.

[6] www.livemint.com/Industry/6JcqKUZpKn1qvqY90zCPVM/Cashless-India-Challenges-and-benefits

[7] economictimes.indiatimes.com/wealth/spend/a-look-at-various-cashless-options

Authors Profile

Dr. Latika Kharb, Professor in JIMS, Delhi, India. She has over 15 years of teaching and 4 years of research experience in IT. She is one of the shortlisted candidate for UGC organized Commonwealth Fellowship tenable in U.S.A (2004). During her teaching services, she recieved several awards. She is also a member of Board of Referees for several International Journals of IT. She is also a guest of honour/ judge/ chair person/organizer for various technical fests, conferences and convocation. Her research areas include: Software Metrics, Software Testing, Artificial Intelligence, Cyber Laws, Bioinformatics to Access Biological Database & Gene Identification, Mobile Computing, Computer Forensic Science, Nanotechnology, CyberMedicine & Dentistry Autonomic Software Systems and many more. She has published more than 70 research papers in reputed international journals including Scopus, Thomson Reuters (SCI & Web of Science) and conferences including IEEE, Springer. She is Convener of many Springer Conferences. She is Editor of Book series with Springer.

Dr. Deepak Chahal is teaching faculty in Department of MCA, JIMS, Sector-5. He has over 10 years of teaching and 3 years of research experience in IT. He has published various research & technical papers in reputed national & international journals. He has been the convener of ICICCT -2016, 2017 & 2018 Technically sponsored by **Springer & CSI.**

