A Survey Paper on Secure Digital Payment

Vaishnavi[1], Jamuna[2], Usha C S[3]

[1]PG Scholar, Dept. of Computer Science and Engineering, Vidyavardhaka College of Engineering, Karnataka, India
[2]Asst. Professor, Dept. of Computer Science and Engineering, Vidyavardhaka College of Engineering, Karnataka, India
[3]Asst. Professor, Dept. of Computer Science and Engineering, Vidyavardhaka College of Engineering, Karnataka, India

---

Abstract - *In the modern world most of the people use e-commerce applications and other application to do shopping and to do various transactions through Debit cards, Credit cards, online banking, Google Pay, PayPal etc. Security is the key element to success of any application. Hence its necessary to preserve privacy and security to our bank account so that our personal and account details will not be revealed to these applications. In the proposed systems digital tokens are used along with the Block chain technology to provide security for our personal and account details. For the same enough evidence is noted.*

***Key Words*: Block chain, Card payment, Digital Tokens, RFID, Cashless**

1. INTRODUCTION

India is a developing Country. Since Our nation is going to be Digitalized Nation, Digitalized Nation means using the concept of Paperless, Cashless. Cashless transactions occur with the help of Credit cards, Debit cards, bank transactions, Google Pay, PayPal etc. Digital payment means paying or transferring money to a person or entity by means of digital mode. A person's record is required to be connected to the advanced wallet to stack cash in it. The meaning of an electronic instalment framework is a method for paying for a products or administrations electronically, rather than utilizing money or a check, face to face or via mail. A case of an electronic instalment framework is Google Pay.

Nowadays block chain technology is coming into existence. Block chain is Internet database technology. It consists of blocks which are interrelated. In these blocks we store the data. RFID tags are devices that have read only chip which is used to store unique number. It is also called as Radio Frequency Identification. This RFID does not have processing capability. We aim to provide security to the digital payment system. In this paper we discuss about the various methods through which we can make payment.

2. Literature Survey

According to the author ***Balaji rajendran et. Al*** it is suitable to introduce Digital tokens to protect and provide privacy and security to the intermediary system using cryptographic principles. DTE supports the transaction between the remunerator and receiver. In this methodology the customer requests the digital tokens from bank. If there is sufficient amount in the account then the digital token exchanger will provide the tokens to the customers, else tokens will not be generated. We can request the DTE for any number of tokens we want. Using these tokens the customer can make payment to any person or to the entity. The validity of this token is only three months. After the validity period of the token we can remit the token. The Advantage of this proposed model is scalable, practical, and straightforward to implement by the prevailing payment intermediaries. [1].

According to the author ***Alexander Schaub et. Al*** Reputed frameworks should be security protecting so as to work appropriately. Building a reputed system that is security saving with no trust suppositions is certifiably not an easy task, So the author proposes a model block chain with blind signatures. Blind Signature is a form of digital signature where the content is disguised before it is being used. Examples of blind systems are cryptographic election systems, digital cash schemes. Reputed systems would be extremely important, in light of the fact that there is a lot less hazard that the protection of the clients could be ruptured. Such a reputed framework for online business applications, is recommended as security is guaranteed. The advantage in this system is the security is guaranteed as we are using blind signatures along with the block chain concept [2]

According to the author ***T.Chai*** et. Al current systems suffer from security and privacy issues, especially in financial applications. So, the author proposes token based block chain technology. It has three concepts they are Universal token structure, Authirazation Management and Token based booking method. Ethereum adopts account-based accounting method. To enhance the scalability Etherum introduced smart cards. Bit Coin adopts UTXO and POW which supports transactions of currency and exhibits less scalability and low efficiency. To avoid these problems the author proposed block chain and system based on tokens. It provides high security and it requires verification from the owner in each n every step. Advantage of this token system is it will resist attack from new users, prevent attacks from old users and it avoids global rollback. Disadvantage of the system is it is difficult to implement unified token structure of complex scenarios.[3]

According to the author Thomas ***S. Heydt-Benjamin et. Al*** secure payment can be done through RFID. In spite of a large number of RFID-empowered installment cards as of now available for use, all the cards analyzed are vulnerable to security attack. After figuring out the mystery conventions between RFID-empowered charge cards and readers, authors option to manufacture a gadget equipped for mounting a few progressed replay attacks under research center conditions. Major advantage of using RFID is it is cheap when compared to other assests. While supreme security and protection in a contactless-card structure factor may be difficult to achieve.[4]

According to the author ***Ari Juels et. Al*** using RFID technology we can secure the payment system. It is amazing how an unobtrusive gadget like a RFID tag, basically only a remote tag, can offer ascent to the complex challenge of security and protection issues that we investigate here. RFID protection and security include rich exchange among numerous orders, as signal preparing, equipment configuration, inventory network coordinations, security rights, and cryptography. Most of the articles treated in this review investigate security and protection as an issue between RFID labels and readers. Obviously, labels and readers lie at the edges of a RFID framework. Advantage of using this technology is they can track the business assests. A large number of the specialist information security issues like verifying perusers to servers include effectively recognizable information security conventions. [5]

According to the author ***Divyan Munirathnam Konidala et. Al*** a security saving Pre- Paid Mobile HTTPS-based Payment model is best. Thier proposed versatile installment model utilizes rising innovations like the cell phone, RFID, and NFC. The proposed installment model furnishes the client with complete control on his/her installments and security insurance from both the bank and the dealer. The purchaser can drop, get new unknown prepaid money transfers at whatever point and any place he/she needs, utilizing the cell phone's 3G/4G. Advantage is it is similar to a pre-paid card where we can recharge how much ever we need and use it whenever we want. Disadvantage of this system is an update can cramp your style [6].

According to the author ***Scott D. Mainwaring et. Al*** e-wallets are best for digital payment. e-wallets have a long-haul potential for gathering and arranging receipts in a messiness free (or if nothing else less mess full) way, on the off chance that those things could be made incompletely (through labeling) or completely computerized. Such a framework could empower new sorts of complimentary gifts, while likewise giving clients all the more dominant and tasteful approaches to jump over and remain over the memories of urban life. the main advantage in this methodology is it provides access to different types of cards. It is simpler to use. The disadvantage of this methodology is it requires continuous maintenance and updates.[7]

According to the author ***Yanpei Chen et. Al*** Organizations like National CSS started offering reasonable calculation for organizations. The author explains that using cloud computing data can be stored securely. Time-sharing in the long run offered approach to PCs, which carried moderate calculation to the overall population. Along these lines, distributed computing as of now offers moderate, enormous scale calculation for organizations. They will avoid distributed computing from turning into a purchaser item. Similarly as the item PC and the Internet realized the Information Revolution, and made data all around open, reasonable, and helpful, so too clouds figuring can possibly achieve the Computation Revolution, in which enormous scale calculations become all around open, moderate, and valuable. [8]

According to the author ***Yuvaraj Sharma et.al*** Block chain methodology should be used in the payment transactions. The appropriation of new innovations is regularly delayed because of delicate financial issues. Be that as it may, a great deal of regard for new businesses and organizations are moving towards the utilization of uses of digital money and blockchain in the budgetary division. By utilizing decentralized innovation, firms would have the option to defeat value-based charges, accidental charges, and booked expenses while executing card exchanges. Based on the basic correlation between the current installment biological systems and the new pervasive installment framework, one might say that Blockchain innovation could be useful for firms and clients. Advantage is by embracing Blockchain, organizations could increase different focal points with the end goal that quicker business forms execution, decreased exchange cost and foundation costs and conquer odds of digital assaults. Disadvantage is improved straightforwardness, security and decreased cross border exchange expenses and time are the central point that have constrained a few banks and huge partnerships to join blockchain administrations into their rundown of tasks.[9]

According to the author ***Parekh Tanvi et.al*** we need to use mobile phones rather than token for providing strong authentication. The potential outcomes to utilization of cell phone rather than security tokens for solid confirmation. Static secret phrase is no longer secure and effectively powerless for aggressors. Security token can be effectively broadening the confirmation quality however extra cost, single use and server synchronization become most weakness issues. Here SIM based authentication will be done and based on SIM, dynamic password will be generated. To generate the dynamic password, we make use of password algorithm that generates 24 bit dynamic password for each request. GSM Gateway will be used to send the password to the customer. Further, equipment token is given to each client for the individual record which builds the quantity of conveyed tokens and the expense. Advantage is assembling and looking after them, has become a weight on both the customer and association. [10]

3. CONCLUSION

Digital payment is necessary for each and every transaction nowadays as the country is opting for cashless and paperless. To get success to any application security is the key element and authentication is the way to prove that factor. Reputed systems should work properly in order to gain the trust of the people as well as to gain the popularity. So it is very important to develop an application through which we can make secure transactions by not revealing our details to the entity or to the payer. In this survey paper we discussed privacy preserving reputed systems for various applications hence this literature survey will be helpful for the people who plan to build a secure transaction application.

REFERENCES

[1] Rajendran Balaji, Pandey AK, Bindhumadhava BS, "Secure and privacy preservicy digital payment." 2017 IEEE SmartWorld, Ubiquitous Intell Comput Adv Trust Comput Scalable Comput Commun Cloud Big Data Comput Internet People Smart City Innov.

[2]Schaub A, "A Trustless Privacy-Preserving Reputation System A trustless privacy-preserving reputation system". 2019;(November), Springer International Publishing, 2016.Conference.

[3] T. Cai, Hao Wang, Xiji Cheng3, And Linfeng Wang, " Analysis of Blockchain System With Token-Based Bookkeeping Method", Special Section On Smart Caching, Communications, Computing And Cyber security For Information-Centric Internet Of Things

[4] Heydt-benjamin TS, Bailey D V, Fu K, Juels A, Hare TO. "Vulnerabilities in First-Generation RFID-enabled Credit Cards", Proceedings of eleventh international conference on financial cryptography and data security.

[5] Juels, Aris, “RFID security and privacy: A research survey”, IEEE Journal on Selected Areas in Communication 24(2) (2006)

[6] Konidala, Divyan Munirathnam, et al. "Resuscitating privacy preserving mobile payment with customer in complete control." Personal and Ubiquitous Computing 16.6 (2012):643-654

[7] Scott D. Mainwaring, Ken Anderson, and Michele F. Chang, " What's in Your Wallet?Implications for Global E-Wallet Design ", April 2-7 | Portland, Oregon, USA

[8]Chen, Yanpei, Vern Paxson, and Randy H. Katz. "What’s new about cloud computing security." University of California, Berkeley Report No. UCB/EECS-2010-5 January 20.2010 (2010): 2010-5.

[9] Mr. Yuvraj, Dr. Dhiraj, Miss barka sharma,"Blockchain – Creating positive vibes in the Card payment industry",Annual Research Journal of SCMS.

[10]. Tanvi P, "Token Based Authentication using Mobile Phone", 2011 International Conference on Communication Systems and Network Technologies.