# Public Key based Security Scheme for Digital Payment Transactions

M.Ramesh Kumar[1], R. Ganapathy Subramanian[2], M.Arun[3]
[1,2]*Assistant Professor, Department of Computer Science, Mannar Thirumalai Naicker College, Madurai, India*
[3]*Assistant Professor, Department of Computer Science, Sri Krishna Adithya College of Arts and Science, India*

***Abstract*** **- The digital payment landscape in India is undergoing a massive transformation. Indian consumers have shown tremendous affinity to digital technologies, with growth rates for mobile phones and e-commerce adoption far outstripping rates in developed economies. More than 40% of the users of digital payment systems are worried about chances of loss of money during the transactions as well as about the fraudulent activities that happen often in the field. So, continues security enhancement is the only way to reduce the fraudulent activities and give the better user experience. The paper addresses such issues and proposes a better enhancement for the existing digital payment technologies by using public key cryptography-based two-step signature verification scheme.**

***Index Terms*** **- Blockchain, cryptography, publick-key security.**

## I.INTRODUCTION

The digital payments ecosystem in India has come of age in recent years with the pandemic fast-tracking the process of digital payment adoption [1]. An increased number of citizens, even those residing in non-metro cities and India's hinterlands have begun to make the shift to cashless transactions through methods such as Unified Payments Interface (UPI), Aadhaar-enabled Payments System (AePS), Internet Banking, and more. According to a report by KPMG [2], India is expected to witness a 78 per cent increase in digital payments in the upcoming months.
However, as the country gravitates towards more digital payments, it is important to understand the challenges that come along with it. One of the biggest challenges and most important aspects when it comes to digital payments is security. In today's tech-powered world, strengthening cyber security to build a secure digital payments ecosystem is imperative. On that note, let's take a look at how and why digital payment security has become mandatory in today's world.
Public-key encryption is asymmetric encryption because the sender and receiver are not using the same key to encrypt and decrypt. There are two types of keys used in public-key encryption, the public key and the private key. The RSA algorithm is the one of the most commonly used public-key encryption [3]. The algorithm uses two keys, the private key and the public key for encryption and decryption. The sender encrypts the message with the receiver's public key, which is known by everyone, and then the receiver decrypt the message with the private key which is only known by the receiver. In this way, the stand-in attack will be efficiently prevented, that even the attacker captures the message in the middle of the traffic, there is no way for the attacker to decrypt the message since the private of the receiver is needed [4].

## II. LITERATURE REVIEW

In this paper [5], we provide information about the various types of digital signatures that are commonly used in XML transactions. They are also defined a particular schema for storing the result of these operations.
Zhang et al (2011) [6] makes an improvement on digital signature algorithm which is based on elliptic curve cryptography. In this paper he obtained a new digital signature scheme by improving the original digital signature based on elliptic curve cryptosystem. The performance of public key cryptosystems was analyzed through the comparison of two main algorithms: RSA and ECC. The results of the tests

revealed that while both algorithms perform well in terms of key generation and encryption, they are not as fast as one another [7].

In this paper, Kumar et al. [8] proposed a new encryption algorithm that uses the Elliptic Curve. The algorithm is formulated by taking into account the difficulty of finding the right value of k and the random point of the elliptic curve.

## III. CYBER ATTACK AND DIGITAL SECURITY

As the digital payments segment in India achieves rapid growth, fraudulent activities such as hacking, threats, theft, etc., are also on the rise (fig.1). Improving cyber security for secure, encrypted digital payments will allow even marginalised communities, especially those who cannot afford any instances of fraud, to become financially independent. They will no longer need to depend on cash transactions and can utilise digital payment methods, thereby encouraging financial inclusion across the country.

The attackers today are progressively building advanced technologies to target core banking systems especially concerned with payments. Their activities are becoming more and more aggressive and assertive than before to interrupt the victim's capability to respond. They are further collaborating across multiple geographies heightening the attacker's anonymity by requiring no additional resources to carry out the attacks.

Cyber security is the practice of protecting electronic systems like computers etc. and data from malicious attacks. It is also called Information technology security or electronic information security [9]. Cyber security means the body of technologies and practices designed to protect networks, devices etc. from attack, damage from any unauthorized access [10].

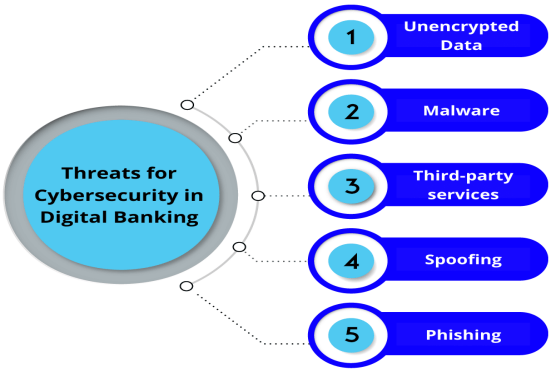


Fig 1. Threats in Digital Banking

## IV. MAJOR ISSUES REGARDING ELECTRONIC PAYMENTS

Digital payment is a good way of making payments online. A tremendous alteration of web-based transactions has occurred with an equal rise in security strikes against electronic payments [11]. Protection in changing the business environment is not readily acknowledged. Electronic payment on the web is a simple target for stealing personal information and money. There are many reasons security vulnerabilities show up in electronic payments. Clients offer charge cards and payment account details along with other private information online. These data are sometimes transmitted insecurely [10]. Electronic payments demand the improvement of information technologies.

A blockchain is a public ledger of information collected through a network that sits on top of the internet. It is how this information is recorded that gives blockchain its groundbreaking potential. Blockchain [1], as its name suggests, consists of multiple blocks strung together. The words "block" (digital pieces of information) and "chain" (stored in a public database). Each block in the network containing the data is secured and connected to each other with the help of cryptography principles Data cannot be changed or altered once recorded in a block, making it impossible to do so without it being seen by the other participants on the network.

Cryptography is used in blockchain as a means of ensuring transactions are done safely, while securing all information and storages of value. Therefore, anyone using blockchain can have complete confidence that once something is recorded on a blockchain, it is done so legitimately and in a manner that preserves security. Integrity of the data is ensured using digital signature, which is the main aspect of data recorded in blockchain Genesis block is the first block of blockchain, contains its transactions that, when combined and validated, produce a unique hash. This hash and all the new transactions that are being processed are then used as input to create a unique hash that is used in the next block in the chain. This ensures that each block links to its previous block through its hash, forming a chain back to the genesis block, so the name blockchain.

## V. TWO-STEP DATA ENCRYPTION

Public-key cryptography requires the public key authentication by a trusted third party called "Certificate Authority". The Certificate Authority plays an important role in issuing, distribution and revocation of public-key certificates corresponding to users' public keys. So, public-key cryptography has the certificate management problem such as distribution, revocation and verification overhead of the certificates.

To prevent our attacks, the SetPublicKey, Sign and Verify algorithms should be modified as follows

- SetPublicKey: For params and $x_i$ , a user $i$ calculates
  $PK_i = (X_i = x_i \cdot P,\ R_i = r_i P)$ -------(1)
  as its public key
- Sign: Given params, a partial private key $D_i$, a secret value $x_i$, and a message $m$, a user $i$ picks a random number $t_i \in \mathbb{Z}_n$ and calculates
  $T_i = t_i \cdot P, k_i = H(m, T_i, X_i, R_i, h_i),\ l_i =$ ----(2)
  $H(m, X_i, R_i, T_i)$,
  $\tau_i = t_i + k_i \cdot (l_i \cdot x_i + s_i)\ mod\ n$

Then $\tau_i$ D $(R_i, T_i, \tau_i)$ is a signature on the message $m$.

- Verify: For params, an identity $ID_i$ , a user public key $PK_i$, a message $m$ and a signature $\sigma_i$ D $(R_i, T_i, \tau_i)$ on $m$, a verifier calculates
  $h_i = H(ID_i, R_i, PK_{KGC}),\quad k_i =$ ------- (3)
  $H(m, T_i, X_i, R_i, h_i)$
  $l_i = H(m, X_i, R_i, T_i),\quad \tau_i \cdot P = T_i +$ ------- (4)
  $k_i \cdot (l_i \cdot X_i + ID_i \cdot R_i + h_i \cdot PK_{KGC})$

If it holds then accept the signature.

In two step verification scheme, the value $R_i = r_i P$ is contained to related to a user's partial private key. If we can set the user public key as $PK_i = (X_i = x_i P, R_i = r_i P)$ instead of $PK_i = X_i = x_i P$ in an improved scheme, since $R_i$ is contained in all signatures. Then, the Type II adversary who knows the master secret key cannot replace the user public key $PK_i = (X_i , R_i)$, the Type II attack to change $X_i$ or $R_i$ can be prevented.

To prevent attack, one can make it impossible for the adversary to replace the public key for the elimination of $PK_{KGC}$. In the Type I attack, an adversary can make $R_i$ or $PK_i = X_i$ so that the part $h_i PK_{KGC}$ related to the master secret key in the verification equation is eliminated. In improved scheme, the public key is $PK_i = (X_i , R_i )$. To succeed the attack, $R_i$ or $X_i$ should contain $h_i PK_{KGC}$ to remove $h_i PK_{KGC}$ in the verification equation. For the verification equation of the improved scheme, $\tau_i \cdot P = T_i + k_i \cdot (l_i \cdot X_i + ID_i \cdot R_i + h_i \cdot PK_{KGC})$, $R_i$ cannot contain the value $h_i PK_{KGC}$ since $h_i = H (ID_i , R_i , PK_{KGC})$ contains $R_i$ as its input. Also, $X_i$ cannot contain the value $h_i PK_{KGC}$ since $l_i = H (m, R_i , X_i , T_i )$ has $X_i$ as its input. It needs $h_i PK_{KGC}$ multiplied by $l^{-1}{}_i$ to eliminate $h_i PK_{KGC}$ in the above equation, but it is impossible to compute $X_i$ so that $X_i$ should contain $l_i$.

## VI. CONCLUSION

Use of digital payment methods such as online banking, digital wallets and other techniques prove to be more efficient in terms of ergonomic factors. The view from a common man's angle suggests that use of digital payments is more efficient and user-friendly with online banking standing next to it in terms of convenience. But security treats is a major worry in the one and it should shot-out. Method of security is continuously evolved but at the same time kind of attacks on the methods. Developers and service providers should ensure users money against the attackers. Two-step signature verification-based security scheme enrich the security of online money traction and provide less chance to attack. This paper discuss in detail about that scheme.

## REFERENCE


[1] Payment and settlement system in India, Technical Document, RBI, 2019

[2] Digital payments analyzing the cyber landscape, KPMG Survey Report 2018.

[3] Salomaa, A. (1990). Public-Key Cryptography. EATCS Monographs on Theoretical Computer Science.

[4] Sekhar, V.C., & Sarvabhatla, M. (2012). A Secure Account-Based Mobile Payment Protocol with Public Key Cryptography.

[5] Opatija, Croatia, XML Digital Signature and its Role in Information System Security by Sandro Gerić, Tomislav Vidačić, MIPRO 2012, May 21-25,2012.

[6] Qiuxia Zhang, Zhan Li, Chao Song, The Improvement of digital signature algorithm Based on elliptic curve cryptography 978-1-4577-0536-6/11/$26.00 ©2011 IEEE.

[7] Kute vivek B., Paradhi P.R., Bamnote G.R., " A International Journal of Computer Science And Applications, Volume 2, No. 1, April/May 2009. Software Comparison of RSA and ECC".
[8] Kumar D.Sravana, Suneetha CH., Chandrasekhar A., "Encryption of Data Using Elliptic Curve Over Finite Fields", International Journal of Distributed and Parallel Systems (IJDPS), Volume 3, No.1, January 2012.
[9] Joshi, K., & Akhilesh, K. (2020). Role of Cyber Security in Retail.
[10] Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cyber security: Threats and Challenges. 2020 International Conference Automatics and Informatics (ICAI), 1-6.
[11] Chun, S.H. E-commerce liability and security breaches in mobile payment for e-business sustainability. Sustainability 2019, 11.
[12] Noor Ardiansah, M.; Chariri, A.; Rahardja, S. Udin The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. Manag. Sci. Lett. 2020, 10, 1473–1480.