SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

3D-SECURITY IN DIGITAL INDIA

Amrita[1], Avnish Shukla[2]

[1]*Guest Lecturer (Computer Science), ANDC, University of Delhi, Delhi, India*
[2]*MCA, JIMS, GGSIPU*

Article DOI: https://doi.org/10.36713/epra10717
DOI No: 10.36713/epra10717

ABSTRACT

Digital India is not just a dream, but it is the need of today's world so that each and every online transaction can be transparent, and secure.

Digitalization is the process of translating information into a digital format to improve productivity and efficiency. Complex information can be represented in a digital format to reach more customers automatically. However, recent cyber-attacks have raised awareness within the Indian digital world for a more pragmatic, anti-cyber terrorism course of action. These may encompass techniques like machine learning and sentiment analysis.

As people in India are less educated and do not have technical knowledge, taking advantage of which hackers do more fraud to them. This paper presents the need for the implementation of 3D-Security and implementing various policies and techniques which assure a safe cyber future and a smooth digital transformation in India.

Through this 3D security, the customers web browser encrypts the information sent between the browser and the merchants web server, using Secure Socket Layer (SSL) encryption. SSL provides high data privacy using a series of protocols. So, confidential details of the user, such as plastic cards, and login details, can be transmitted securely. It also provides data integrity. Unauthorized users can't modify the data. Even if the message is intercepted unauthorized users can't decode the message.

INTRODUCTION

Digitalization [1] is simply a pathway for inducing country digitally authorize in the lea of robotics. India is efficiently forthcoming grove to becoming a digitally progressive country stirred by the diminishing cost and rising availability of Smartphone and speedy connectivity at present, India is pinpointed as one of the bulkiest, thriving markets for digital clients. The Indian government & cyber experts both are functioning 24*7 to make India a secure digital citadel.

Firstly, let us understand what is 3DS? **3DS** is a mechanism used to enhance the invulnerability of automated transactions done by technical and generic digital clients via internet. This mechanism provides full authentication to cardholders and improves the overall performance of online transactions. The 3D Secure system ensures security by providing credit or debit card information directly to the bank and not to the merchant. Information is encrypted and transferred through HTTPS protocol so that the information can be read only by the bank.

NEED OF THE 3D CYBER SECURITY?

Cyber security plays a vital role in terms of the digital world for any country but in the case of India its role is very crucial and mandatory too. In India the online fraud ratio is very high because the Cyber literacy as well as literacy ratio of India is very low as compared to other developed countries. Our people are a very easy victim of any scammer also it is necessary to have strong and strict cyber security. With the massive growth in the use of digital systems over the years, there have been a speedy growth in cyber frauds around the world too. Cyber criminals have grown much more state-of-the-art, making it complicated for organizations to protect themselves towards cyber threats.

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

CYBER CRIME RATE IN INDIA

DIAGRAM 1. BANKING FRAUDS [2]

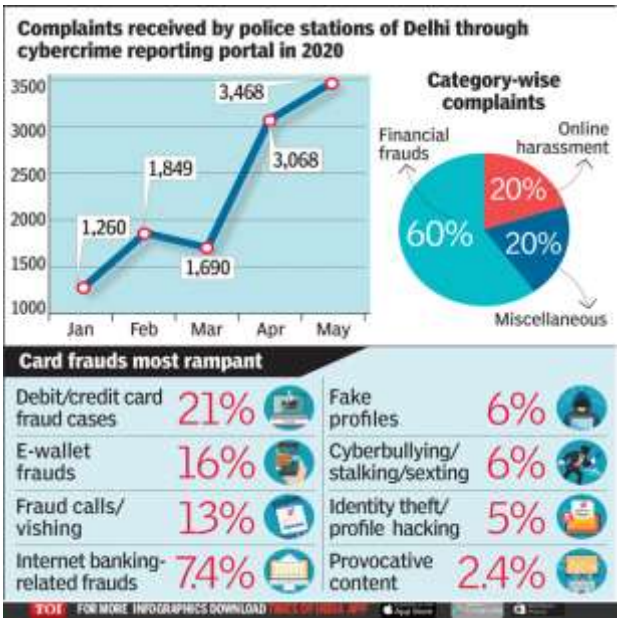

Diagram 2. Financial Frauds [3]

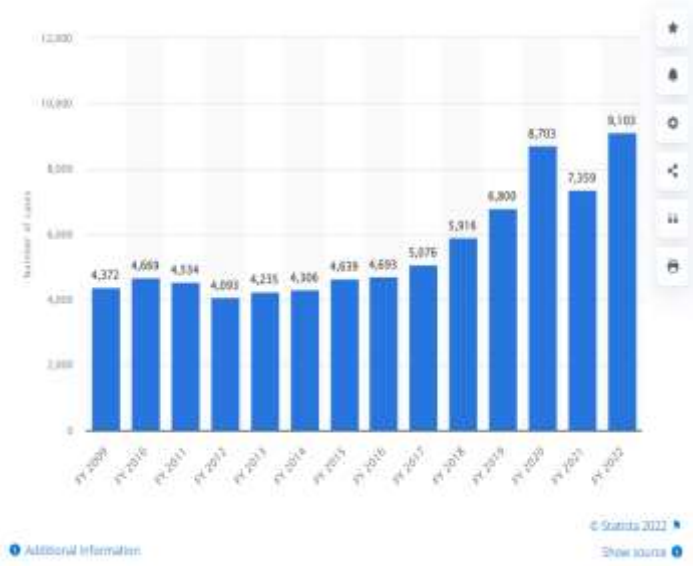

Diagram 3. Financial Frauds Statistics [3.2]

Basically, **3D Security works in 3-Domains as follows**:

- **Issuer Domain** or the financial institution that has issued the card being used for the online transaction.
- **Acquire Domain** or the Merchant/Acquirer to which money is being paid.
- **Interoperability Domain** which is the network being used like Visa/MasterCard.

1) **Acquire Domain** –The acquiring bank processes credit and debit payment on behalf of a merchant. A Merchant enters right into an agreement with the acquiring bank in the shape of merchant account. The acquiring bank exchanges the fund with the issuing bank and ensures that the merchant receives payment for payment card activities. The Acquire domain covers the relationship between the merchant and acquirer.

2) **Issuer Domain** –The issuing bank is the financial institution, bank, or card provider, who issues the card to the cardholder for making online transactions or purchase of any e-commerce goods or services, and their relationship is maintained by issuer domain.

3) **Interoperability Domain** – The relationship between the acquirer and issuer domains is supported by the interoperability domain.

SECURITY REQUIREMENTS FOR ONLINE TRANSACTIONS [4]:

- **Payments Clandestine:** All information about the end-users and every transaction must be kept confidential. During online transmission and storage,

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

this is the decisive service required by each end-user and the merchant is just the service provider.

- **Payment Probity:** During transmission and storage the probity of the transaction must be protected by both end-user and merchants who require this service.
- **Entity affirmation:** These services are required by both end-user and merchants in order to verify the identity of entities with whom they are doing the transaction.
- **Non-Reversible:** This feature provides unforgeable evidence for each and every online transaction, which enables one party to prevent another party from denying the online transactions. For example, sending order payment information for confirmation of order payment, both end-user and merchants also require these services.

3D SECURE

The boom in cellular telephone utilization indicates a clean trend towards Wi-Fi net gadgets and the 3-D secure protocol. Which was designed for the assistance of "net buying", wherein the cardholder is shopping the usage of a web-enabled device and the authentication takes place over the internet. Security is a primary challenge in all challenges in E-trade and especially inside the case of online transactions, with the use of Debit card, Credit card or net-banking. Following the failure of Secure Electronic Transaction (SET), 3-D Secure is emerging industry. The standard for online transaction security [5]. Simplicity and safety are the vital factors for online transactions/protocols to be of the future standard.

3D Secure is **a further** step, which **you'll be able to** enable to have **anytime** when a card transaction **is created** online. It enhances security measures for shoppers and vendors alike. **once you activate** 3D Secure, you'll be asked to validate every transaction **together with your** PIN code.

3D stands for "three domains." **the primary is that the** card issuer; second, the retailer receiving the payment; and third **is that the** 3DS infrastructure platform that acts as a secure go-between for **the buyer and also the** retailer

Available 3D Secure Platforms are: Two main samples of 3D Secure protection platforms are Visa Secure and Master Card Secure-Code. Both use 3DS technology as an extra layer of consumer protection, to shield cardholders from fraud and counterfeiting a fraud.

To check Merchant is 3D secure

To quickly check if a merchant or vendor you're making a payment with is 3D Secure compliant, explore for the Verified by Visa or Mastercard Secure-Code logo on their site.

SUMMARY

3DS is a secure transaction protocol used as an additional level of security utilized for Debit or Credit card or Net Banking transactions. In this paper we stepped forward on how properly the 3DS protocol meets the E-transaction security requirements and identified the risk of deceit during e-transaction. For further research the topic is to analysis the security of E-transactions, efficiency and the performance of the 3DS protocol.

REFERENCES

1. *Towards Digital India Transformation: Pragmatic Implementation of 3-Dimensional Cyber Security Pyramid to Counter Cyber Attacks in India*
2. *https://www.ijeter.everscience.org/Manuscripts/Volume-5/Issue-9/Vol-5-issue-9-M-19.pdf*
3. *Banking frauds:*
4. *https://securityboulevard.com/2021/01/the-rising-online-banking-frauds-in-india/*
5. *Financial Frauds*
6. *https://timesofindia.indiatimes.com/city/delhi/as-people-stayed-home-cyber-fraud-tripled-during-lockdown/articleshow/76699209.cms*
7. *3.2) Financial Frauds*
8. *https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/*
9. *A Secure Electronic Transaction Payment Protocol Design and Implementation*
10. *https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.681.9219&rep=rep1&type=pdf*
11. *3DS*
12. *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.6613&rep=rep1&type=pdf*