IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 5, May 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Applications and Implementation of IoT In securing Online Transactions

Dr.M.N. Nachappa[1], Shubham Jain[2]

[1]. Professor and Head, School of CS ad IT, Jain University, Bangalore

[2]. Graduate Student, Department of MCA, Jain University, Bangalore

Abstract-- In this quick creating world, the utilization of web has given an awful lift to the utilization of electronic mode of performing exercises identified with banking so that everybody needs to go paperless and perform exchanges on the web. Indeed, individuals lean toward making installments of their power charges, versatile bills, water charges travel tickets, and so forth utilizing these electronic mediums. Most importantly, so as to enable the general population to play out these exchanges it is important to make their exchanges more verified and secured so that there is no loss of information just as the cash incorporated into this. What's more, to accomplish this objective there are numerous practices which is being actualized and considerably a greater amount of such things are being found.

Then again, Internet of Things (IoT) is likewise blasting as it makes the human work all the more simple and advantageous. At the end of the day IoT is an arrangement of interrelated figuring gadgets, mechanical and computerized machines, items, creatures or individuals that are given one of a kind identifiers (UIDs) and the capacity to exchange information over a system without expecting human-to-human or human-to-PC connection.

So why not to utilize the idea of IoT in verifying the online exchanges? The utilization of IoT is unquestionably going to result in far superior improvement and make these exchanges more verified for the utilization of overall population.

I. Introduction

Online Transaction are firmly identified with individuals' matter of fact and day by day exchanges. Individuals presently incline toward utilizing on the web installments as opposed to utilizing the money. The past patterns were extremely intricate to keep up records for money exchanges where the general population used to keep up certain registers or some other manual records, and so forth. The fast development of online exchanges with the assistance of IoT will help and make it feasible for verifying these exchanges increasingly secure and dependable [8].

II. Existing Systems

A portion of the current techniques which are being utilized for online exchanges are as per the following [1]:

A. Credit Card

The most famous type of installment for web based business exchanges is through Credit cards. It is easy to utilize; the client needs to simply enter their MasterCard number and date of expiry in the proper territory on the merchant's page. To improve the security framework, expanded safety efforts, for example, the utilization of a card verification number (CVN), have been acquainted with on-line MasterCard installments. The CVN framework distinguishes extortion by contrasting the CVN number and the cardholder's data.

B. Debit Card

Debit cards are the second biggest online business installment medium in India. Clients who need to spend online inside their money related limits want to pay with their Debit cards. With the debit card, the client can pay for bought merchandise with the money that is as of now there in his/her ledger instead of the MasterCard where the sums that the purchaser spends are charged to him/her and installments are made toward the finish of the charging time frame.

C. Smart Card

It is a plastic card installed with a chip that has the client's personal data put away in it and can be stacked with funds to make online exchanges and moment installment of bills. The money that is stacked in the smart card diminishes according to the use by the client and must be reloaded from his/her bank account.

D. E-Wallet

E-Wallet is a prepaid account that enables the client to store numerous credit cards, debit card and bank account numbers in a safe situation. This disposes of the need to enter in record data unfailingly while making installments. When the client has enrolled and made E-Wallet profile, he/she can make installments quicker.

ISSN (Online) 2348 – 7968
www.ijiset.com

Some of the instances of e-wallets that are commonly used are as per the following [4][5][6]:

i. PayTm
ii. Oxygen
iii. MobiKwik
iv. PayUMoney
v. Amazon
vi. PhonePe
vii. FreeCharge
viii. RazorPay
ix. Airtel Money
x. Vodafone mPaisa
xi. Jio Money
xii. ICICI Pockets
xiii. State Bank Buddy
xiv. HDFC PayZapp
xv. LIME
xvi. Ola Money
xvii. PayPal
xviii. Rapido

E. Netbanking

This is another popular way of making e-commerce payments. It is a simple way of paying for online purchases directly from the customer's bank. It uses a similar method to the debit card of paying money that is already there in the customer's bank. Net banking does not require the user to have a card for payment purposes but the user needs to register with his/her bank for the net banking facility. While completing the purchase the customer just needs to put in their net banking id and pin.

F. Mobile Payment

One of the most recent methods for making on the web installments are through cell phones. Rather than utilizing cards or cash, all the client needs to do is send an installment solicitation to his/her service provider by means of instant message; the client's mobile account or credit card is charged for the buy. To set up the mobile payment system, the client simply needs to download a software from his/her provider's website and afterward link the credit card or mobile billing information to the software.

III. Proposed System

Executing IoT in verifying on the web exchanges is an exceptionally urgent advance which should be taken in this as speedy as lightning developing business sector in the fields of online exchanges. These days, even the little retailers just as the road nourishment merchants are utilizing a few or the other kind of online exchange. In this way, the execution of IoT can be a noteworthy advance towards verifying these online exchanges.

A. IoT in Online Payments

To facilitate the shopping knowledge for the purchaser, shippers try to make a frictionless installments experience. The IoT is the main impetus in getting this going. For installments, the IoT implies that a shopper can pay in practically any manner conceivable.

Some of the case that can be considered are as per the following:

i. Rather than a card, shoppers could pay with their mobile, a wearable, a vehicle, or a voice-initiated gadget ("Alexa, request me a pizza."). For organizations, this implies empowering things other than a standard in-store terminal to approve installments. The IoT expands the network between things without the requirement for human mediation.
ii. The requirement for installments to be handled consequently applies to both the B2B and B2C universes. A shrewd cooler could recognize when you have to purchase milk, make the request, and have it conveyed, all without you never lifting a finger. A business can purchase a printer that tracks toner use and requests by means of Amazon once it achieves a specific dimension. The utilization cases are unending.
iii. Consider when a shopper signs into a versatile application like Apple Pay. The client can make in-application buys while never having to reemerge their MasterCard data. Buyers can likewise pay with unique mark distinguishing proof, enabling them to make buys in a flash.

Applications, for example, this are rapidly turning into the standard, however for them to work effectively, data should be remained careful.

B. Securing Data in IoT devices

Alongside the numerous advantages of the IoT, the danger of a security rupture can't be disregarded. With so much data shared crosswise over numerous gadgets and things, it is unavoidable that programmers will attempt and gain admittance to this valuable data.

We can adopt some of the accompanying measures to guarantee the security of our important information in the IoT gadgets, especially when we are utilizing it in online transactions:

i. Use of PCI Compliance [2]
ii. Use of tokenization technique
iii. User Authentication
iv. Linking tokenization to user authentication

ISSN (Online) 2348 – 7968
www.ijiset.com

IV. METHODOLOGIES

A. Use of PCI Compliance

As payments became electronic, a gathering of overwhelming hitters from inside the payment industry (AMEX, Discover, JCB, MasterCard, and Visa) united to make Payment Card Industry Data Security Standards (PCI DSS).

These models guarantee that all organizations that procedure, store or transmit charge card data keep up a safe domain. That incorporates all traders, merchants, or programming suppliers who handle charge card data.

There are four different levels of PCI-Compliance based on transactional volume [3]:

Level 1. Any vendor – paying little heed to acknowledgment channel - preparing over 6M Visa exchanges every year. Any shipper that Visa, at its sole attentiveness, decides should meet the Level 1 trader prerequisites to limit hazard to the Visa framework.

Level 2. Any vendor – paying little respect to acknowledgment channel – handling 1M to 6M Visa exchanges every year.

Level 3. Any vendor processing 20,000 to 1M Visa e-commerce transactions per year.

Level 4. Any vendor preparing less than 20,000 Visa internet business exchanges every year, and every single other shipper – paying little mind to acknowledgment channel – handling up to 1M Visa exchanges every year.

Depending upon the scale of transactions, one can choose the level of compliance which is compatible with the device.

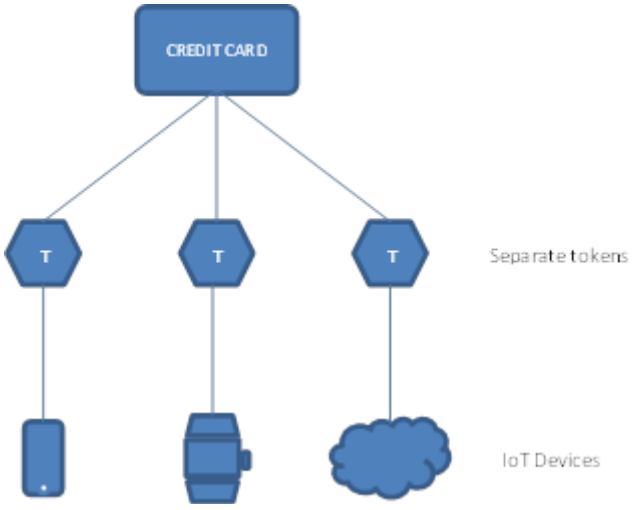
B. Use of tokenization technique

Tokenization, when connected to information security, is the way toward substituting a sensitive information component with a non-sensitive comparable, alluded to as a token that has no outward or exploitable importance or value. The token is a reference (for example identifier) that maps back to the sensitive information through a tokenization framework. The mapping from unique information to a token uses strategies which render tokens infeasible to turn around without the tokenization framework, for instance utilizing tokens made from arbitrary numbers [9].

There are several techniques through which we can achieve tokenization. One of the technique which I suggest is of generating tokens based on the devices where the token will be used.

We can use some custom API's to generate the tokens from the device which we will be using for making payments. The generation of such tokens will ensure that the online transactions are taking place from the device from where the token was generated previously.

The below diagram explains the flow of the generating tokens from the devices and ensuring the same at the end point where the payment is collected.



As shown in the above figure, there is a separate token generated for every individual device where the credit card (in this case) is used. These tokens are generated for dedicated devices and only works for those devices. The generated token is also sent to the merchant. While confirming the payment both these tokens are compared and if both are same, then only it will accept and confirm the payment.

We can include this mechanism in each and every IoT device where we want to include security in our online transaction.

C. User Authentication

Authentication is the demonstration of affirming reality of a characteristic of a solitary bit of information guaranteed valid by a substance. Interestingly with identification, which alludes to the demonstration of expressing or generally showing a case purportedly verifying someone or something personality, verification is the procedure of really affirming that character [10].

There are two main types of user authentication factors:

i. Single factor - As the weakest dimension of authentication, just a solitary segment from one of the three classes of variables is utilized to authenticate a person's character. The utilization of just a single factor does not offer much assurance from abuse or malevolent interruption. This sort of authentication isn't suggested for monetary or actually applicable exchanges that warrant a larger amount of security [11].

ii. Multi factor - It includes at least two authentication factors (something you know, something you have, or something you are). Two-factor authentication is an uncommon instance of multi-factor authentication including precisely two factors [11].

ISSN (Online) 2348 – 7968
www.ijiset.com

D. Linking tokenization to user authentication

The general idea driving a token-based authentication framework is basic. Enable clients to enter their username and password so as to get a token which enables them to get a particular resource or operation - without utilizing their username and password. When their token has been acquired, the client can offer the token - which offers access to a particular resource for a timespan - to the remote site.

As it were: include one dimension of indirection for authentication - rather than validating with username and password for each secured resource, the client authenticates that route once (inside a session of restricted length), gets a time constrained token consequently, and utilizes that token for further authentication amid the session.

By using this technique we can merge 2 separate yet powerful measures to make a single methodology which makes the security even stronger and reliable.

Other than these 4 methodologies mentioned above, there are numerous methodologies which can be used to make the increasing online transactions more secured and reliable with the use of IoT.

V. Conclusion

By utilizing the techniques talked about above, we can attempt to coordinate IoT in performing on the web exchanges and that too with some improved well-being and security of the information put away in those IoT gadgets.

VI. References

[1] https://services.amazon.in/resources/seller-blog/different-types-of-e-commerce-payment-systems.html
[2] https://www.investopedia.com/terms/p/pci-compliance.asp
[3] https://learn.na.bambora.com/understanding-pci-compliance/
[4] https://www.feedough.com/e-wallet/
[5] https://marketbusinessnews.com/financial-glossary/e-wallet/
[6] https://www.thewindowsclub.com/best-mobile-wallets-in-india
[7] https://learn.na.bambora.com/understanding-tokenization/
[8] https://www.tatadocomo.com/business/downloads/WhitePapers/resources/The-internet-of-shopping-how-iot-can-transform-shopping-malls.pdf
[9] https://en.wikipedia.org/wiki/Tokenization_(data_security)
[10] https://en.wikipedia.org/wiki/Authentication
[11] https://www.miracl.com/user-authentication