IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 15, Issue 2, Ser. II (Mar-Apr 2020), PP 32-39
www.iosrjournals.org

Secured Online Transaction (SONT):Analysisand Solution Of Secure Electronic Transaction.

Ihedioha Uchechi. M[1], Onyedeke Obinna C[2], Dr. Ezema Modesta [3], Agubata Immaculate Chidinma[4], Uzo Blessing Chimezie[5]

[1]*Department of Computer Science, University of Nigeria, Nsukka*
[2]*Department of Computer Science University of Kairouan, Tunisia.*
[3]*Department of Computer Science, University of Nigeria, Nsukka*
[4]*Department of Computer Science University of Kairouan, Tunisia.*
[5]*Department of Computer Science, University of Nigeria, Nsukka*

Abstract:*Online transactions are gradually taking over conventional trading methods, thereby becoming a logically accepted exchange medium. A lot of financial and economic burden is now lying on the Internet crux. A foremost security threat to online transactions today is cybercrime attacks. Therefore, this work deals with the concept of Secured Online Transaction (SONT). In so doing the paper investigated some available cyber Security measures and their roles in Security of Online Transactions. The various highlight of this paper is on online transaction securities. The work developed an algorithm which is called SONT that define the processes representing a secured online transaction ranging from customers, banks and merchants with a protection against fake electronic card details. The method used is by introduction of variable keys that validate card holders and merchant details from issuer before authorization using two-way verification.*

Keywords*: Cybercrime, Internet, Secured Online Transaction (SONT), Online Interface (OI), Electronic Card*

Date of Submission: 25-04-2020 Date of Acceptance: 08-05-2020

I. Introduction

It is very necessary to secure online transactions as they are becoming most applicable means of purchasing goods and services. Without security of the platform it will record a decline in patronage and eventually fizzle out. The major objectives of this work are itemized as: concept of Secured Electronic Transaction, identify Information Communication Technology (ICT) security branches and review cybercrime protection acts on Critical infrastructure security and, illustrate a Solution secured algorithm in performing secure online transaction called SONT. We have different protocols used in secured online transaction such as SET, iKP, KSL, and 3D secure protocols but Diffie-Hellman is a popular agreement protocol in payment protocols and is the most famous key agreement protocol. Secure electronic transaction (SET)is an open encryption and security requirement for online transaction. The function of this protocol is to shield electroniccard dealings over the Internet. Previously, SET was developed as result of security challenges arising inuseby MasterCard and Visa in February 1996 [1]. Just like there is no water tight system, SETexhibits some flaws, exposing cardholders to vulnerability of deceitful merchants who over billtheir prey customers with more than their advertised price; hackers and phishers that set up illegal Uniform Resource locator (URL) to sieve electronic card information [1]. In the same way, the merchants are not properly protected from fraudulent customers who do vice versa with the provision of prototype credit and debit card records or claim refunds without a genuine failed transaction [2]. The provision of law that protect customers in SET, makes merchant appear to be more vulnerable to fraud, as done in most of the countries in the world.Secondly, we identified that several fundamental SET application implementation issues [3].

Why is SONT necessary in today’s technology? SONT can be defined as secured online transaction and as in SET above. It is aimed at mitigating the pitfalls of SET.

The Trust means that all parties should have digital certificates and the privacy defines that information or any details is made available only when and where necessary. Cybercrime remain a threat to Internet users and is on the great increase. Majority of Internet users assume that they are untouchable when surfing the net, without knowing that it is impossible to be completely safe while performing online transactions. However, we can implement some simple measures to help increase our web security.

Different attempts to define and classify cybercrime as undertaken by scholars, intergovernmental organizations, government agencies and private businesses [4] and further categorizes cybercrime also as those crimesharnessed by the application of Internet technology and computer devices.

In a resolution from the Council of European Cybercrime,they outlined cybercrime as any fraud ranging from illegitimateactionsmade in contradiction to data integrity. Cybercrime is any crime perpetrated by the use of computers, computer networks, or hardware devices according to [5]. Cybercrime is a new wave of crime that is highly competing with illicit drug dealer'strade. The cybercrime system now comprisesof researchers seeking more dangerous attack methods, hackers who compromise databases and rend them vendors vulnerable [6]. Space transition theory is doing its best to contribute to the field of cyber criminology in particular [7].

One of the major medium online transactions in today's jet life is ATM (Automatic Teller Machine). Minimally, long banking queues are being converted by the channel of ATM machine. A secure online 24 hours self-banking service has made the ATM the crux of the banking system. Availability of ATM assist the user to perform his usual banking activities both cash and cashless transactions making it possible to pay various utility billssuch as electricity, water, and phone seamlessly. ATM has proved to be a convenient and light means of carrying out various banking transactions in a jiffy [8]. As the use of ATMs has been increasing day by day the number of fraudulent attacks on the ATMs also increases. The ATM design prescribed fraudsters to the devising of stealing cards, the cloning of cards and some other cyber-crimes [9]. An ATM card authenticates persons after it verifiesthe card details of the intended user [10]. In their work [11] recommends a chip which works for fingerprint recognition system administered for recovery in case of a stolen card. [11] Biometric technology provides secure and irrefutable authentication. Here at the start fingerprint of persons is registered in the database using fingerprint module. There are 4 switches used in registering the fingerprint of the persons. The then16x2 LCD display is used to display whether person is authorized or not but the fingerprint module will recognize fingerprint of the persons and will transfer this data to Arduino, Arduino will further send a signal to the GSM module. [11]

II. Progressive Analysis of Online Transaction Security.

In order to understand the concept of online transaction, Credit Card, Debit Card, Prepaid Cards and other online payment platforms generate.

A Credit Card is a plastic chip in a rectangular shape used to buy goodsand services,which helps to acquire cash withdrawals on credit terms. It is acredit without collateral or security. [12] The assignment of a re-usable Card makes it possible for the holder to purchase with limit and re-pay in full or partially. Just as in the case of a credit Cardholder can pay his debt in full to avoid high interest repayment.Electroniccardis a safer means than cash and is also becoming most preferred payment method internet-wide.

This card payments that have been pre-paid offer a credit scheme. Although there are still different types of credit cards used in different ways [13], they often work the same way as debit cards. Online Payment is an electronic payment, which is supported by other payers or checks between banks for online transactions in real-time.

When comparing Orthodox payments, we find realized that online transaction systems are easier, faster, more efficient and more economical. Each user can complete the payment process anytime via the internet.Third payment is available as a debit card to review and assist in bank and mortgage transactions.

We have a third party payment mode which serves like a credit intermediary to supervise and support between online interfaces and the bank [14]. It is important to note that there are conditions which are vital in making business organizations to gain trust on security technologies in the delivery of online transactions, and also manage such technologies by using the Secure Sockets Layer (SSL) protocol.

Information and Communications Technology (ICT) security solutions will be discussed below.

[15] Cybercrime chat rates have been reported on companies as well as on local and global economies, with cyber security officials resorting to the basics to inspire policy makers to take the lead in combating cybercrime. Therefore in identifying of problem facing the security of online transaction. There is an increasing number of internet users from decades to decades, year to year in significant percentage.

Significantly one can say that a great version of the population is exposed to the risk of cybercrime. Security of online transaction is of great essence having considered the percentage of internet transactions per day. It is therefore important that this work will be significant to internet security experts and the scholars of internet technology.

Most of the times, the business organization or transacting customer is led to believe in a false sense of security. Having sound background knowledge in the security building block helps prevent this illusion. In the same vain, it is also exactly this sense of security that prospective online customers are searching for, and willing to believe in in secure business organization when security is involved.

[16]Believes that law enforcement agencies have failed in the account for the various risks associatedwithgateway and access systems.

In this work criticized Africa as a continent for dealing slackly in the area of cyber security with its private sectors not excluded. Nigeria is also a hit in this flaws. The South African government is spear heading the cyber legislation to address cybercrime [17]. However, the Nigerian cyberspace is under threats [6]. National critical infrastructure (NCI): As defined by the Oxford dictionary “Infrastructure” as the basic physical and organizational structures and facilities that laid out the need for Critical Infrastructure protection and the nation’s policy response. The U.S. Senate is also on top of itformulatingcyber security legislation. The government’s track record does not absolutely guarantee safety on cyber security [18]. The United Kingdom (UK) follows a similar approach”.

The Centre for Protection of National Infrastructure (CPNI) lists nine sectors that form part of National Infrastructure in UK. In the UK the Cabinet office is the nodal agency responsible for Cyber security. The UK identifies cyber as a Tier One risk as part of its National Security Strategy (UK Government, 2010) and calls out cyber-attacks by other nation states, terrorists or organized crime as a priority.

Governments at all levels have paid very little attention to the protection of critical infrastructure. [19] It is important to note that there are conditions which are vital in making business organizations to gain trust on security technologies in the delivery of online transactions, and also manage such technologies by using the Secure Sockets Layer (SSL) protocol.

Online platforms over the internet creates an enabling environment for different parties to advertise and execute transactions within themselves. However, online transactions will only be popular if the public trusts in its security.

Significantly one can say that a great version of the population is exposed to the risk of cybercrime.

Our study on the percentage of internet transactions per day reveled the need for security of online transactions. This work will be beneficial to the scholars of internet technology and security experts. Year 2018 recorded a high-risk result of cybercrime [16].The cyber security industries have also added to the bottom line as a motivator infight against cyber-crimes.

Therefore, in relationwith problem facing the security of online transaction. Most of the times, the business organization or transacting customer is led to believe in a false sense of security. Having sound background knowledge in these Security building block helps the prevention of this illusion.

In the same vain, it is also exactly this sense of security that prospective online customers are searching for, and willing to believe in: an interface that really negates the threat of cybercrime by inclusion of cyber security.

2.1 AVAILABLE CYBERSECURITIES

Critical infrastructure Security: The focus here is on the study of cyber threats and the threat of the Nations. Broadband penetration is becoming affordably suitable for Internet users. As a result, Africa is slowly becoming a "safe haven" for cyber criminals. We can say that African countries are more in a hurry to deal with things as poverty, financial crisis, and fuel crisis, lack of policies, racial problems and traditional crimes such as murder, rape and theft. As a result, this attack on cybercrime is already a hit. In this wise ICT awareness should not be made public because of the lack of proper regulation required to combat cybercrime at the national and local levels, which has led to problems with cybercrime. At the same time, some African countries are trying to deal with cybercrime [20]. The important role we seek for the proper use and commitment of social, political and technological relations in Nigeria, as well as the new millennium sources, is moral corruption.

Recently, the Federal Government of Nigeria introduced a law before the National Assembly to legislate that Telecom programs are stored within the country and designated as a valuable public safety as an application that can prevent network security and protect unauthorized access to the network [21].

Cloud security: This is a series of policies, technologies, resources, and controls used to protect the network infrastructure (such as IP quality, data, resources, services, etc.). Information security requires the control and importance of effective and effective payment processing technology. Internet services [21].

Application security: Thisdefines security steps at the application level. E-commerce security systems have this benefit of today’s world, such as online banking or other businesses around the world which are online transactions. [21] This security includes built-in security measures, such as an application firewall that defines real-time tasks and hacked tasks based on application security protocols (including programs such as periodic tests).

IoT security (internet of things security): IoT security protects devices connected to the Internet of Things (IoT) network. Each "thing" is uniquely identified. Working on the Internet provides new features for online banking, but it also brings many new risks [21]. Simply allowing devices to connect to the Internet exposes them to many vulnerabilities that are not properly protected**.**

Point-of-sale (POS) security: POS security prevents fraudsters from gaining unauthorized access through payment. Through the SET system, the POS application is also essential to communicate with the payment gateway installed on the receiving bank server [3]. From a security perspective, these two interpretations deserve special treatment [21].

III. Methodologies

The basic Building Blocks of Services in cyber security based on encryption, digital signatures and message authentication codes (MACs).
An understanding of these basic concepts evolved in secured online transaction. SONT verifies any order by the use of variable keys which function as a 2-way factor authentication key to ensure customer order and security.

Distributed Database System for Credit Card Transactions Mirroring:

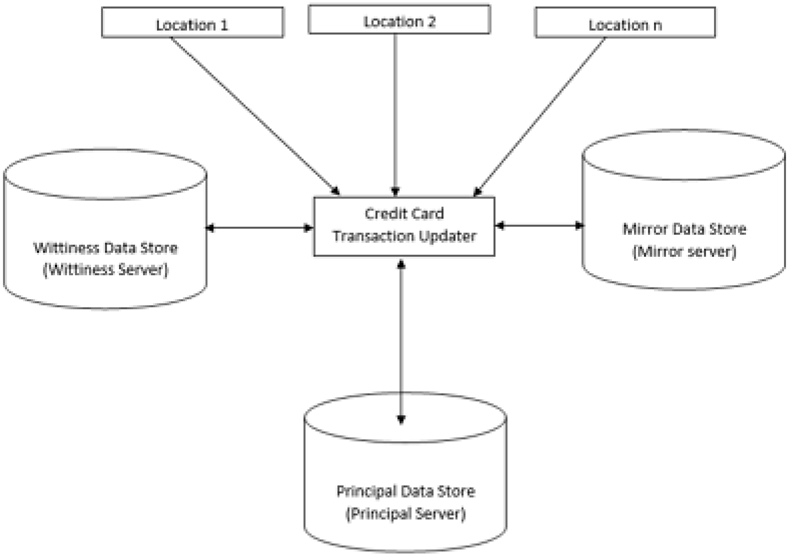

Figure 1

Mirroring sometime called Shadowing, is the process of creating multiple copies of data and database. In mirroring, we copy database into different machines or locations. If any primary server smashes,then the system can transferto the mirrored database automatically. Tight coupling between the mirrored and primary database is established with the assistance of relationship blocks of the transactions log to the reflected database. Just in case of any failure, it's co-jointly capable of reestablishing the information by recapping it from one database to another. Once any failure takes place, the mirrored database becomes the principal information.

Location: is different credit card access point by customers to make transactions. The location n means any giving Automated Teller Machine, POS and Internet Transaction.
Transaction Updater: Have access to the different database at the same time in a real time approach manner.
Wittiness Date Store: is a database server for comparing the data of other existing data store to determine the actual information of the credit card bearer to avoid fraud activities. It is called the recovery data store
Principal Data Store: is database server known as the principal server, it is the actual credit card transaction database system.
Mirror Data Store: could in mirror database 1…. n, this actual refer to data store switcher from a particular mirror data store to another.

3.1 WHAT ARE SONT REQUIREMENT

These are the requirements of SONT: provide personal information about the process and payment, ensure the integrity of all shipping information, and ensure that Credit Card holder is genuine and provides a guarantee that the Seller can receive trade proceeds via the credit card. SONT key functions are as confidential as information, data integrity, credit card verification and Merchant verification.

Participants in the SONT program are Cardholders, Bank on Hold (Issuer), entrepreneur, commercial bank (Merchant). Encryption, of course, involves the process of converting personal information seen as mockery into an impossible code writing. It also includes a hash-hash collection of payment codes. Payment rules include: original account number, including new tools to prevent expiration (EXNonce) [21]. In order to regain the original plaintext, the reverse process called decryption must be performed.

Decryption of the cipher text typically depends on a key that is secret and authorized parties only know them. This ensures that a password or key is encrypted only, only the authorized parties can decrypt the information, since only them knows what the secret decryption key is. Encryption methods performance is commonly of two types, namely secret-key encryption and public-key encryption.

3.2 INTERACTION BETWEEN CUSTOMER, MERCHANT, BANKS AND ISSUER OF THE PROPOSED SYSTEM

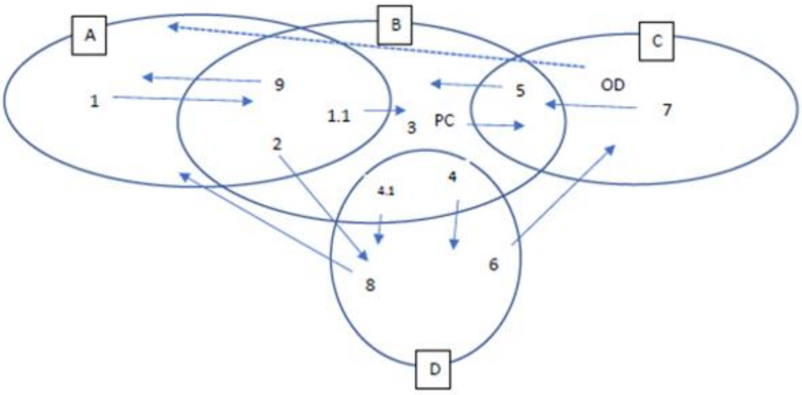

Figure 2: flow diagram with nodes and links shows the interaction levels between the participants

As in algorithm below, the flow diagram with nodes and links shows the interaction levels between the participants their intersection and their union as well.

A = CARD HOLDER
B= ONLINE INTERFACE
C = MERCHANT
D= BANKS (ISSUER, MERCHANT AND CUSTOMER BANK)
PC= PAYMENT CONFIRMATION,
OD=ORDER DELIVERY

Table 1

In a re-modelled relationship diagram, we obtain below. Nine steps for this protocol simplified below.

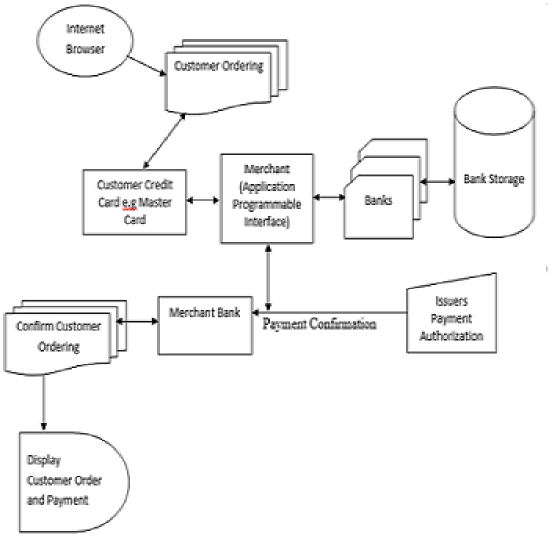
Internet Browser
Customer Ordering
Customer Credit Card e.g Master Card
Merchant (Application Programmable Interface)
Banks
Bank Storage
Confirm Customer Ordering
Merchant Bank
Payment Confirmation
Issuers Payment Authorization
Display Customer Order and Payment

Figure 3: A simplified nine steps including database as Storage

We refer to table 1 in this explanation of this remodeled relationship diagram.

1. In a bid to do a trade, A browses the internet.
2. A, therefore transmits transactions details
3. Transaction details includes

a. C’s pan Tran
b. C’s bank (involves the 2-Factor verification)
4. C sendsCard information (3b) to their D
5. C’s bank depends on issuer for payment pass
6. Issuer sends authorization to the C’s bank
7. C’s bank sends authorization to the merchant
8. C will complete ODto A and also captures the transaction from their D
9. D prints invoice for A.

3.3MATHEMATICAL ALGORITHMS FOR STEP 3

Using Main article: Hash chain, we put below the Hash chain mathematical expression for this model generation.
This one-time password system works as follows:
1. Chosen a starting value.
2. Apply hash chain function f(s)
(For n times) obtaining a value of: f (f (f (.... f(s) ...fn.))).
3. At first login, Userobtainsfn-1(s).
4. It follows suit with in next login, as fn-2(s).
5. Keephashing with this reduction.as previous login.
[22] Talking about the S/KEY one-time password system we obtain that observed that it is derived OTP based on Lamport's scheme. In some mathematical algorithm a static key can be provided to be used as an encryption key by only sending a one-time password. [22] In order to use thechallenge-response in one-time passwords there is a need to provide a response to the challenge. [22] Speaking of the S / KEY one-time password system, we found that it was obtained from OTP based on the Lamport method. In some mathematical algorithms, a static key may be provided for use. [22]

3.3 LIMITATION

Our work tried to show the interactive flow diagram and to develop and implementable algorithm. This paper can be enhanced by further research with the ability of working hand in hand with Card issuers to bring it in a commercial use. We are limited in our small scale of recognition for now. It is also worth to state that there is no water tight system and as such, we encourage further contributions, critics and advancement to this work.

IV. Result And Conclusions

```
ALGORITHM FOR SONT EVENTS
Step 1
      1.1 Define card holder as Customer
              1.1.1 Define Customer Card Issuer as Issuer Bank
       2.1 Define Merchant
               1.2.1 Define Merchant's bank As Acquirer
                      1.2.1.1 Obtain Merchants details
 1.3 Define Online Interface as payment gateways

Step 2
        2.1. Customer browses the web
        2.2 Customer decides to purchase
                2.2.1 Inputs Card Details into interface
                2.2.2 The Online interfaceliaises with the SONT to confirm the details
Step 3
       3.1 SONT will send order and payment details to Merchant Bank
       3.2 The Online interfaceliaises with the issuer to confirm the details
           3.2.1 If details are yes
        3.2.1.1 The Online Interface reconfirms with the Card holder Using 2-way level factor
                3.2.1.1.1   1st level check confirmation on SMS, if yes then, proceed to
                3.2.1.1.2   $2^{nd}$ level check via goggle authentication; if yes
                        3.2.1.1.2.1 Then provides a link to continue
                3.2.1.1.4   If No decline and abort transaction Else
3.2.1.1.2   Yes amount is withdrawn from his account
Step 4
```

```
4.1   Fund is cleared by an intermediary clearing Bank house
      4.1 Fund is deposited into the Merchants bank account
      4.2 Merchant captures transaction
      4.3 Merchant confirms payment
      4.4 Merchant sends supply transaction details to the online Interface
      4.5 Merchant supplies services to the customer
      4.6 Merchant completes the order

Step 5
          5.1 Acquirer sends credit card bill to customer
Step 6 Order Successful
End.
```

The idea of indemnity defines sections covered by merchant in case of any breach.

The Merchants are liable or free from lapses depending on the terms and definitions. The Card User, merchants and Issuers exists but the major factor is human role or responsibility. Machines can fail but most of the times we garbage in and garbage out

Above all we recommend that carefulness be inculcated towards employee training and re-training as they form the weakest link in the cluster of card issuance and physical management.It is easy to gain access by using someone’s valid credentials. This is because a staff that has transaction approval profile can be easiest and least-detectable way to gain unauthorized access to networks and data. However, it is highly advisable to keep investing wisely in security. Keep deploying right technologies as time keeps evolving.

It is important to note that attackers will always launch and the response to it by organizations will assist to reduce, limit orevencompletely eliminate the damage intended.

References

[1]. Mohammad Vahidalizadehdizaj, Avery Leider Seidenberg, 2017, “Mobile Payment Protocol 3D by Using Cloud Messaging” Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 5th, 2017 School of CSIS, Pace University, Pleasantville, New York

[2]. Vahidalizadehdizaj, M, A. Moghaddam, R and Momenebellah, S, 2011,” New mobile payment protocol: Mobile pay center protocol (MPCP),” International Conference on Electronics Computer Technology, vol.2, no., pp.74,78, 8-10 April 2011

[3]. Pita Jarupunphol, Wipawan Buathong, 2013, “Secure Electronic Transactions (SET): “A Case of Secure System Project Failures” IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 2013

[4]. Fawn Ngo, Jaishankar K, 2017, “Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime” International Journal of Cyber Criminology Vol 11 Issue 1 January – June 2017. 1-4

[5]. Gordon. S, Ford. R, 2006,“On the definition and classification of cybercrime” Journal of Computer Virology, 2, 13-20.

[6]. Odumesi, John Olayemi, 2014 “Combating the Menace of Cybercrime” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 980-991

[7]. Holt, T., Bossler, A. M, 2016,”Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses”. Abingdon, Oxon: Routledge

[8]. SNaga Gowri, RDurga Devi and PGowshalya, 2017, “A Biometric based ATM Security System using RFID & Rajput Shivam Kumar et al.; International Journal of Advance Research, Ideas and Innovations in Technology”, International Journal for Modern Trends in Science and Technology, Vol. 03, Issue 04, April, pp. 169-176.

[9]. Chaitali Bhosale, Pooja Dere, Chaitali Jadhav, Feb 2017,"ATM security using face and fingerprint recognition", International Journal of Research in Engineering, Technology and Science, Vol. VII, Special Issue,

[10]. Archana A. Talikoti, Deepa Modi and Laxmi Talikoti, 2018,"SECURITY OF ATM SYSTEM USING RFID AND OTP", Visvesvaraya Technological University, Belagavi,

[11]. S. K Rajput, A.R Patne, A. Varma andG. Vishe 2019, “Enhanced fingerprint recognition and OTP to improve ATM Security” International Journal of Advance Research, Ideas and Innovations in Technology ISSN: 2454-132X (Volume 5, Issue 2

[12]. Raisa Delwar, 2018, April, “Credit Card Operations of Eastern Bank Ltd. and Opinion of Credit Cardholders About EBL’s Credit Card Service Quality” The Internship Affiliation Report Faculty of Business School BRAC University, Available http://dspace.bracu.ac.bd/xmlui/bitstream/handle/10361/10330/14364009_BBS.pdf?sequence=1&isAllowed=y

[13]. Bello. A. B, Ahmad I.T, 2014, “Security Enhanced Online Registration Prepaid Scratch Card Payment Approach” Journal of Engineering and Technology Research, 2014, 2 (6):53-59

[14]. Baike. 25.06.2017. “Third-Party online payment”, Cited: 10.02.2020. https://baike.baidu.com/item/%E7%AC%AC%E4%B8%89%E6%96%B9%E6%94%AF%E4%BB %98

[15]. Sampath Kumar Venkatachary, Jagdish Prasad and Ravi Samikannu,2018, “Cybersecurity and cyber terrorism - in energy sector – a review” Journal Journal of Cyber Security Technology Volume 2, 2018 - Issue 3-4

[16]. Harold Abelson,1 Ross Anderson et al, 2015 “Keys under doormats: mandating insecurity by requiring government access to all data and communications” Journal of Cybersecurity, 1(1), 2015, 69–79 doi: 10.1093/cybsec/tyv009

[17]. Fawzia Cassim, 2011 “Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players” The Comparative and International Law Journal of Southern Africa Vol. 44, No. 1, pp. 123-138

[18]. Paul Rosenzweig, 2012, “The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government” The Heritage Foundation leadership for America, No. 2695 | May 24, 2012.

[19]. Ken Nwogbo, 11 January 2019,“worrying security situation of critical infrastructure”, https://guardian.ng/business-services/communications/worrying-security-situation-of-critical-infrastructure Assessed 13/12/2019

[20]. Warwick Ashford, 2018, “Top 10 cybercrime stories of 2018” https://www.computerweekly.com/news/252454146/Top-10-cyber-crime-stories-of-2018, computer weekly.com, assessed on 10/02/2020.

[21]. Raju.B, Anjana.J. D, Gulfishan F. A And Jyoti. B, 2010, “The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology” (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 1, April 2010

[22]. L. Lamport, 1981 “Password Authentication with Insecure Communication”, Communications of the ACM 24.11 (November 1981), pp 770-772

Ihedioha Uchechi. M,etal. "Secured Online Transaction (Sont): Analysis and Solution Of Secure Electronic Transaction." *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* 15(2), (2020): 32-39.