IOT BASED FRAMEWORK FOR SECURITY PREVENTION FROM VARIOUS ATTACKS ESPECIALLY IN ONLINE E-TRANSACTION

Shraddha Jaiswal
Sushil Kumar Maurya

ABSTRACT

Security in a range of E-commerce applications includes an efficient framework for information security, namely for computer security, data security, and other online transactions. A secure and scalable transaction depends on an e-commerce application's security. Among these are features of security-integrity, privacy, non-repudiation, and secrecy. As a result, several security techniques are created to guarantee the safety of online transactions in e-commerce apps. Although these security algorithms work well and defend against many attacks, it's important to take data storage during transactions and algorithm calculation time into account. Some problems still need to be addressed, like: Increasing the Use of Computational Cost at the Client and Server Side; and Security Prevention from Various Attacks during Online Transactions in Web Mining, Particularly in E-commerce Applications. The present architecture that has been suggested for protecting online e-transactions in web applications is efficient in terms of computing parameters and provides security against various types of assaults. The suggested design provides security protection against a range of risks, especially for IoT. The method used here validates the user's legitimacy by giving them a challenge value. As a consequence, we believe that our proposed framework will be more effective and successful.

KEYWORDS- *Information Security, IoT, Computer Security, E-commerce, Authentication.*

INTRODUCTION

The measurements document two workers who developed an innovative, low-entropy, communal subversive (a watchword) that served as the basis for a shared, cryptographically strong important. In this case, the objective is to stop offline terminology events, when a malevolent entity systematically records possible phrases on its own and tries to match the precise phrase to use that is deemed acceptable. That is, if offline sessions are not sufficiently prepared, a PAKE strategy is vulnerable, and the greatest protection is an online language dose where an adversary must deliberately try to mimic a genuine meeting using every conceivable phrase. These kinds of online dosing are distinct in the setting of password-based authentication; moreover, wait staff can identify them as failed login attempts and adjust their protocols appropriately. Under the auspices of a competition, protocols for robust key disagreement enable two parties to work together to produce a self-doubting agreement and to harvest a shared, cryptographically durable significant [20]. These are some of the most important and often used cryptographic primitives; in fact, before smoothly developed activities such as encoding and communication verification become practicable, it is better to have a standard technique. Using two workforces, PAKE measures generate a shared, cryptographically robust key based on a creative, low-entropy, underground community (a keyword). When off streak numbers are not employed, a PAKE approach is unfairly imperiled. An online vocabulary fight is a popular illustration of this, where an opponent must actively attempt to emulate a genuine group by employing every watchword that may be used. The watchword-founded authorization standard includes online variants of this instruction; more notably, they may be blocked aside by waiters who recognize them as attempts at unsuccessful logins [21]. Most watchword-based user verification providers put all of their faith in the verification agent, who keeps watchword confirmation data or keywords in a readily accessible folder in a conspicuous location [3, 19]. Traditional watchword-based confirmation techniques depend on a single waitron that supplies all the proof (watchword, for example) required to authenticate an operator. Watchword grounded corroboration is the most widely used item confirmation approach since it requires no secured stowage and enables an operator to verify anyplace, at any time, using only a watchword. Most of the existing watchword-based proof systems initiate the single waitron norm when a lone waiter happens in a community. The worst-behaved single waiter tradition is for the waiter to view one act of destruction for a little period of time, believing that their reconciliation would expose all the watchwords used to manipulate that the waitron has intercepted. The following are a few popular methods for watchword confirmation [2, 5]:

A. Two Servers Password Authentication

Two server confirmation tools are carefully guarded to provide user authentication in an Internet-based secure environment. The number of operators who want to use several operational amenities grows along with the number of operational amenities that are provided on a daily basis. A memorability problem has arisen from the difficulty of remembering many employer (uniqueness) ID/watchword combinations when every demand is met, requiring the operator to function at the greatest level independently. A two-server password authentic key arrangement tool with watchword is designed for this regular usage to find the employer's secret key. The two real-world waitron watchword verification and key exchange organizations are protected against unconnected glossary doses when adversaries get proficient with waitrons [8, 10].

B. Quantum Channel for two Server Password Authentication

In order to verify the accuracy of a conference significant and to check for listeners, important key circulation methods in important cryptography utilize theatrical instruments to disseminate meeting answers and community debates. Nevertheless, group talks need additional channels of communication between a communicator and an earphone and use valuable quantum bits. The important based two server keyword authentication process flow, which draws inaccessible, explains our design of a two server keyword scheme positioned using the quantum key classical approach to efficiently store user passwords in online applications. The finest illustration of this two influence confirmation structure is our present ATM system, where the PIN number is an additional influence and the ATM card is one influence. Therefore, in the event that the ATM pass is lost wages, the validation capacity will become unusable. Regarding biometrics, this organization's sanctuary is just as efficient and productive; yet, personal worries mostly arise from the expense of expensive hardware and software.Earnings from a fragmented vocabulary indicate bargaining for the waiter. Much politeness has recently been incorporated into clever watchword-based real crucial debate procedures that are impervious to any kind of interference. To address this challenge, a creative confirmation assembly was arranged, baptizing the many waiter confirmations. In these multi-server confirmation scenarios, the modest stance that users find most pleasant is the two-server confirmation protocol [1] [4].

C. Two Server Systems

Using a manipulator ID and watchword is a sensible and systematic strategy. Identifying and allowing access to the property of the authorized operator is one of the unique and essential characteristics of a confirmation organization [7]. A solitary waitron organization is one in which the watchword is maintained in a single waitron. There are a few problems nearby, even if the confirmation structure is centered on a single waiter. The independent waiter business is open to several forms of external assaults. The main advantage of the hostile waiter arrangement is that the impostor may irritate the company by trying every explanation until they cooperate. A thorough examination may also be advantageous, as Fig. 1 illustrates.

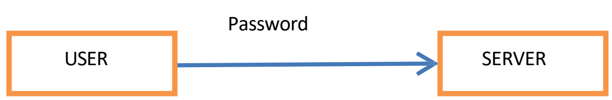

Fig 1: Block Diagram of a Single Server System

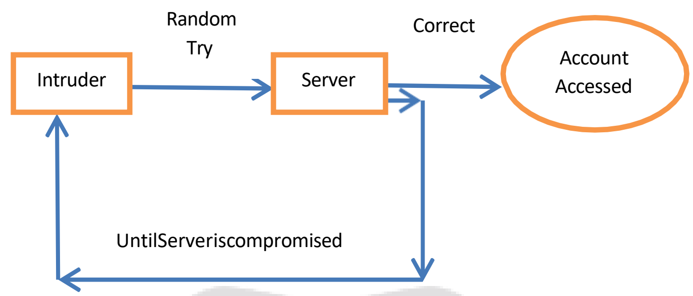

Fig 2: Example of single server system hacked by Intruder

Thus, it is essential to comprehend the idea of two waitron confirmation organization. Negotiations are easier for attackers when there is just one waitron organization. But in the two waitron groups, the aggressor would not be able to just bargain.

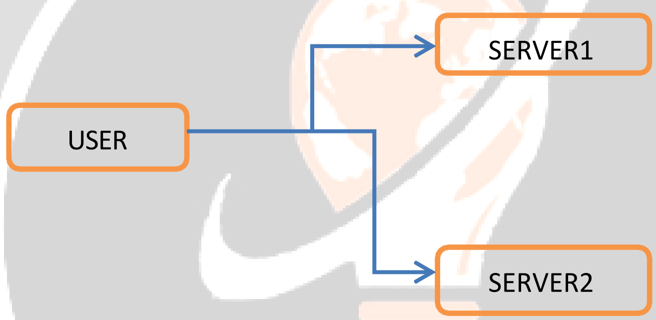

Fig 3: Block Diagram of Two Server System

LITERATURE REVIEW

Now, let's discuss research initiatives by S. Bellovin and M. Merritt, who reported the first encrypted key exchange technique that was successfully password-authenticated. The most reliable and durable variants of EKE successfully convert a shared keyword into a collective key that can be used for encryption and/or message verification, despite the fact that many of the early techniques had flaws. With the use of real key exchange protocols, two parties may collaborate over an unpredictable network while creating a shared, cryptographically strong key while being fully monitored by an opponent. These are among of the most important and often used cryptographic primitives; in fact, establishing a shared key was required even before it was possible to do more complicated operations like encoding and memorandum confirmation. Genuine, important communication techniques based on watchwords record two operators to gain a shared, cryptographically resilient key that originated with an initial, low-entropy common element (a watchword). Katz, Ostrovsky, and Yung (KOY) developed the first well-organized PAKE process with a resistance of refuge in the conventional perfect [6]. Unorthodox in their approach were Gennaro and Lindell (GL), who offered an overall design that incorporates the new KOY procedure as a special instance. These procedures are protected seamlessly under coordinated presentations by the same group, but they need a shared orientation thread. In PAKE, where mutual strictures may be hard oblique into an application of the etiquette, even if it may be less pleasant than the simple classical, dependence on a CRS does not seem to be a purposeful disadvantage in repetition. In order to achieve common confirmation, the KOY/GL outline requires a CCA protected encoding arrangement (such as the Cramer-Shoup cryptosystem with a connected straight projective hash meaning) and its postponements need four rounds in command. The KOY/GL framework may be seen as being expanded upon and built upon in almost all later attempts on a well-structured PAKE in the traditional form. The first acceptable refuge classical for true key exchange conventions between two celebrations was created by Wanga, Z. Cao, K.-K. Choo, and L. Wangthe [9]. The latter has been extended to security assessments of the aforementioned two-party password-based key exchange, employing idealized assumptions such as the random oracle and the ideal cipher models. Provably safe two-party password-based solutions have recently been created in the usual classical environment. Although three-party password-based protocols were discussed in literature, none of their schemes offered substantiated security. In fact, our whole design seems to be the first provably secure three-party password-based genuine key exchange mechanism.

D. XiaoFei and M. ChuanGui[11] provide more relevant study, which is an authenticated key debate in the three-party location. To this extent, the primary effort consists of Needham and Schroeder's actions, which supported the group that disseminated Kerberos. Later, Bellare and Rog became familiar with the architecture of the primary grounded key circulation arrangement that is provably safeguarded, so familiarizing themselves with the required refuge conventional length techniques in this particular situation. This week, we look at the rare but important case when the hidden rationales come from a small ethical code. Such an approach is expected to lead to extensive cooperation, according to Yang et al. [16]. Interestingly, several refinements and conflicts in conceiving this kind of arrangements, distinct from the outdated watchword based confirmation, are revealed after finishing the refuge analysis of Yang et al.'s arrangement. Yang & al.'s structure, which represents a disjointed watchword predicting occurrence in Supplement A, nevertheless falls short of achieving its desired primary refuge goalmouth. However, the adversary method proposed by Yang et al. imprisons the accurate two influence corroboration of clever card-based keyword authorization preparations: a user can only fully communicate out the smart-card-based keyword authorization procedure with the isolated corroboration waitron if they possess both the accurate keyword and the cunning card. Xu, J., Zhu, W., and Feng, D.[17] created a broad construction agenda that included changing the conservative, provably protected PAKE procedures to creative card-based forms and purposely designing an imaginative arrangement to verify its efficacy. In order for the new building to fulfill all of their goals, they want it locked. We will clarify in the next part that the main purpose of their outline is to disconnect keywords that predict events, so removing power and ensuring that the new structure remains secure even in the unlikely event that the enemy finds the secret data kept on the smart card. Zubaile Abdullah, MadihahMohd Saudi, and Nor BadrulAnuar introduced a cutting-edge and successful technique for mobile botnet detection using the Proof Concept [18]. An impenetrable understanding of bot systems' operation and the current research on the best ways to identify and counteract mobile botnet activity are given in this article. A nasty botnet movement has been revealed by the analysis of the Cruse Wind Botnet Cipher using stationary research techniques and opposing manufacturing progress.

METHODOLOGY

- Each time a new customer completes an online transaction, they have to use a shared challenge value to shake hands with the server via a secure connection. The consumer and server shake hands based on the challenge value and secret shared password. The value of the Challenge is unique to that particular Session.
- After First Factor Authentication, the Customer has to register on the server and authenticate using Second Factor Authentication. This phase consists of several procedures, such as registration, login, verification, and password changing.

A. First Factor Authentication using Challenge Handshaking

During an online transaction, the client sends a request to the server, which receives a response from the server. The server asks the client to enter a challenge value. The server establishes a master key using the MD-5 hashing technique in response to the challenge value and requests the client's unique password. Since every client has a different password, the client computes a master solution and replies to the server with the challenge value and password after inputting the password. The server verifies the client's identity and verifies both keys.

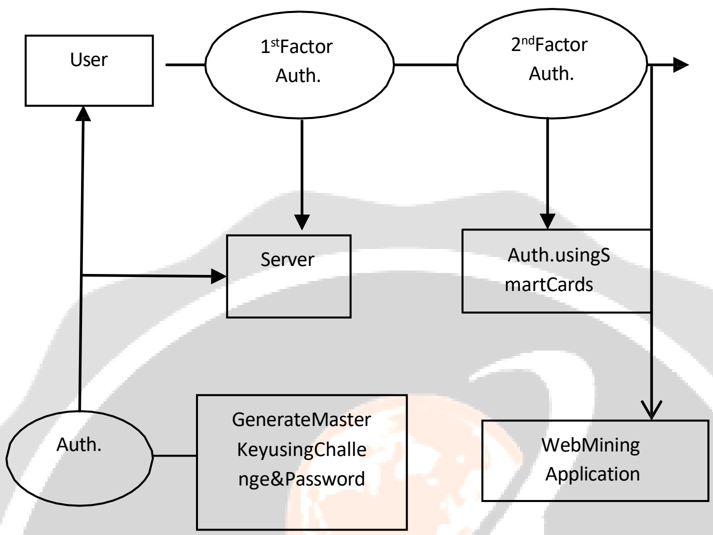

Fig 4 : A framework of Proposed methodology

Algorithm 1

1. The client will initially ask the server for the computed challenge value.

2. The Web Transaction Server will accept the Challenge Value.

The Time Stamp T1 is determined by the server.

4. The server will now get the password value.

5. The server sends the client a challenge value with the time stamp T1.

6. The client thereafter obtains the Challenge Value and Time Stamp T1 from the server.

7. After that, the client determines T2, or the current time stamp.

8. Using these Time Stamps T1 & T2, the consumer calculates the overall transmission time.

$T\boldsymbol{U}tunbmiei\boldsymbol{U}nntime = 2 * (T2 - T1) + paWcessiiragtime$

Using the challenge value, password, and total transmission time, the consumer may now determine the MD5 hashing algorithm.

10. The client calculates an MD5 hash using this information.

11. The client will provide this information to the server.

12. The server receives data D1 from the client and computes timestamp T3.

13. Challenge value + password + T3 are decided by the server.

14. The server also determines the MD5 hashing on (challenge value + password + T3).

15. If they match, the session is valid. Verify whether the password is still operational.

16. If a valid send is accepted but an invalid send is rejected, the session ends.

17. In the event that the session ends, the client will indicate.

18. The validity of the password, if it hasn't expired.

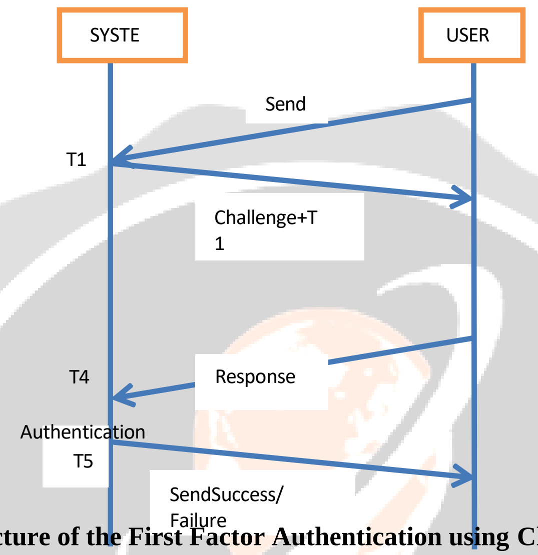

Fig 5: Architecture of the First Factor Authentication using Challenge Handshaking

B. Second Factor Authentication using Improved Smart Cards

As part of the second factor authentication procedure, smart cards are utilized for single server registration. Asymmetric encryption is used for sending and receiving high-level security transactions.

The various Annotations used in the algorithms are as follows:

Table 1: Various Annotations used in Algorithm

Customer/Client	Ui
Server	S
CustomerID	IDi
Customer Password	PWi
Hash(.)	OneWayHash functionsuch asMD-5/SHA-1/ SHA-256
‖	Concatenation
Xor	Xoroperation
X	SecretekeyofServerS
Tu	Transmissiontime
ΔT	Differenceintransmissiontime

C. New Client Registration Segment

During the registration step, the client Ui must record in the inaccessible server S. IDi and PWi are the primary information provided by the consumer. The recording consultant previously determined the hash values (IDi) and (IDi||PWi) and sent instructions to the unavailable server S over a secure frequency. Using an elliptical curve-based solution and characteristic-based encoding, the computed values are sent to the server encrypted. Following receipt of User UI's registration claims, the server verifies the message by using his public key to decode the contents. Server S investigates the same user interface-related issues. S calculates

$$PA_i = Hash(ID_i).xor.hash(X_s||hash(ID_i))$$

$$PB_i = PA_i.xor.hash(ID_i||PW_i)$$

$$PC_i = hash(PA_i)$$

$$PD_i = hash(ID_i||PW_i).xor.hash(X_s)$$

and added a certain amount to the elegant tag memory before sending Client Ui this elegant certificate. Client Ui receives this smart certificate via a secure network.

$$PA^* = PBi.\ xor.\ hash(ID^*||PW^*)$$

Furthermore, the comparison between PCi* and PCi, which are created in the lovely card memory, is confirmed by PCi* = hash (PAi*). If not, the process is deemed too repetitive. As an alternative, Client Ui can be accepted as the rightful owner of the tidy certificate. On the other hand, tag generates an arbitrary nonce Ri by computing.

i

$$PE_i = PA^*.xor.PR_i$$

$$PC_{id} = hash(ID||PW).xor.PR_i$$

$$PF_i = hash(PA_i||PD_i||PR_i||T_u)$$

Upon receiving a request from a client, Tu becomes the active instance. knead {PFi, PEi, PCid, Tu, hash (IDi)} then pushes the login demand to the unavailable server S.

b. Confirmation/substantiation segment

Following receipt of the login application notice for {PFi, PEi, PCid, Tu, hash (IDi)}. The server authenticates the authority of the time barrier between the current (Tu') and previous times, where Tu' is the journey time of the message or data. The difference time (ΔT) is the product of the current time (Tu') and the prior time (Tu), and it represents the predicted convincing time distance for a communication hurdle. Following submission, the appeal is either accepted by the server and sent to the subsequent phase, or it is rejected.

Server calculates –

$$PA_i^* = hash(ID_i).xor.hash(X_s||hash(ID_i))$$

$$PR_i^* = PA_i^*.xor.PC_i$$

$$G = hash(ID_i||PW_i)^* = PC_{id}.xor.PR_i$$

$$PD_i^* = hash(ID_i||PW_i)^*.xor.hash(X_s)$$

And computes

$$PF^* = hash(PA_i^*||PD_i^*||PR_i^*||T_u)$$

and verifies the equivalentity of PF and PF*. Reject the filed appeal if it is not identical. The current time (Ts) is an isolated server in a progress instance, and server S computes PFs = hash (hash (IDi) || PDi || PRi || Ts) someplace if they are identical. After that, the recognize message {PFs, G, Ts} is sent to the user's Ui. Following receipt of the concede message by the smart card, it computes

$$G^{*} = hash(IDi||PWi)$$

$$PF^{*} = hash(hash(ID\ )||PD\ ||PR\ ||T\ )$$

determines if the parameters (G) = G* and PFs = PFs*, as well as the reciprocal substantiation progression, are same. This is where the server and client reauthenticate with each other. If they match, then the server and the client collaborate via tags to create the conference solution (Sk).

$$S_k = hash(hash(ID_i)||T_s||T_u||PA_i$$

Otherwise dismiss to over entering progression.

c. Secret code modifies Phase

This step is included each time Client U has to replace the password (PW) with a more complicated password (PWnew). Next, Client U wishes to modify the secret word by entering his newly constructed smart card, new (ID*), and new (PW*). The tag then verifies the equivalentity of parameter (C) = C*. If this is true, Client U is the rightful owner of the tag. Tag, however, asks that the new code word, PWnew, be used in the client Ui. After the new secret word is bound inward, the tag calculates

$$B_{new} = PA_i.xor.hash(ID_i||PW_{new}) \text{and}$$

$$D_{new} = hash(ID_i||PW_{new}).xor.hash(ID_i||PW_i).xor.PD_i$$

CONCLUSION

Security in various e-commerce applications includes an efficient basis for information security, especially for data and computer security and other Internet of Things applications. A secure and scalable transaction depends on an e-commerce application's security. Among these are features of security-integrity, privacy, non-repudiation, and secrecy. As a result, several security techniques are created to guarantee the safety of online transactions in e-commerce apps. Data must be stored throughout transactions and while the algorithm is computing, even if these security methods are strong deterrents against attacks. Consequently, an efficient method is implemented that provides efficient computational cost and time together with security for online e-commerce transactions.

The Two Factor Authentication framework, which provides security against threats, especially in the Internet of Things, is the foundation of the planned procedure that is being carried out here. The implemented approach works in two phases: in the first, the user's validity is ascertained by assigning a challenge value; in the second, improved smart card-based authentication is used. The proposed approach provides defense against security-integrity, non-repudiation, confidentiality, privacy, and other threats. Additionally, it defends against a variety of security flaws such as replay, identity theft, and external attacks.

REFERENCES

[1]XunYi,"Security Analysis of Yang et al.'s Practical Password-Based Two-Server Authentication and Key Exchange System", 4th International Conference. Network and System Security (NSS), 2011.

[2]N. Kuruwitaarachchi, P.K.W. Abeygunawardena, L.Rupasingha&S.W.I.Udara, "A Systematic Review of Security in Electronic CommerceThreats and Frameworks", Global Journal of Computer Science and Technology: E Network, Web & Security Volume 19 Issue 1 Version 1.0, 2019.

[3]HayaAlshehri, FaridMeziane, "The Influence of Advanced and Secure E-Commerce Environments on Customers Behaviour: The Case of Saudis in the UK," in 12th International Conference for Internet Technology and Secured Transactions, 2017.

[4]Jiang Huiping. “Strong password authentication protocols”,4th International Conference Distance Learning and Education (ICDLE),2010.

[5]Dr. Happy Agrawal, Moon MoonLahiri, “Gender Influenced Online Shopping Behavior among College Students”, Purakala (UGC Care Journal), Vol-31-Issue- 55-June -2020

[6]J. Katz, R. Ostrovsky, and M. Yung: “Efficient And Secure Authenticated Key Exchange Using Weak Passwords”. Journal of the ACM, 57(1):78–116, 2009.

[7]ShuoZhai,“Design and implementation of password- based identity authentication system”, 2010International Conference Computer Application and System Modeling (ICCASM), 2010.

[8]Harold NguegangTewamba, Jean Robert Kala Kamdjoug, Georges Bell Bitjoka, Samuel FossoWamba, Nicolas NkondockMiBahanag, “Effects of Information Security Management Systems on Firm Performance”, American Journal of Operations Management and Information Systems, volume 4(3): pp. 99-108, 2019.

[9]S. Wanga, Z. Cao, K.-K.Choo, and L. Wang, "An improved identitybased key agreement protocol and its security proof," An International Journal of Information Sceinces, vol. 179, pp. 307-318, January. 2009.

[10]PuspaIndahatiSandhyaduhita, "Supporting and Inhibiting Factors of E-Commerce Adoption: Exploring the Sellers Side in Indonesia," in International Conference on Advanced Computer Science and Information Systems, 2016.

[11] D. XiaoFei and M. ChuanGui, "Cryptoanalysis and Improvements of Cross-Realm C2C PAKE Protocol,"WASE09, procedings of IEEE, International Conference on Information Engineering, pp. 193-196, 2009.

[12]Abdul Gaffar Khan, “Electronic Commerce: A Study on Benefits and Challeges in an Emerging Economy,” Global Journal of Management and Business Research:

B Economics and Commerce, vol. 16, no. 1, 2016

[13]SomdechRungsrisawat, ThanapornSriyakul, KittisakJermsittiparsert, “The Era of e-Commerce & Online Marketing: Risks Associated with Online Shopping”, International Journal of Innovation, Creativity and Change, Volume 8, Issue 8, 2019.

[14]Cong Cao, Jun Yan, Mengxiang Li, "The Effects of Consumer Perceived Different Service of Trusted Third Party on Trust Intention: An Empirical Study in Australia," in 14th IEEE International Conference on e- Business Engineering, 2017.

[15]SomdechRungsrisawat, WatcharinJoemsittiprasert, Kittisak Jermsittiparsert, “ Factors Determining Consumer Buying Behaviour in Online Shopping”, International Journal of Innovation, Creativity and Change, Volume 8, Issue 8, 2019.

[16]Pu, Q.,”An improved two-factor authentication protocol”. In: 2010 International Conference on Multimedia and Information Technology (MMIT). vol. 2, pp. 223– 226.Ieee, 2010.

[17]Xu, J., Zhu, W., Feng, D.:” An improved smart card based password authentication scheme with provable security”. Computer Standards & Interfaces 31(4), 723– 728, 2009.

[18]Abdullah, MadihahMohd Saudi and NorBadrulAnuar, “Mobile Botnet Detection: Proof of Concept”, 2014 IEEE 5th Control and System Graduate Research Colloquium, 2014.

[19]Ghada El Haddad, EsmaAimeur, HichamHage, "Understanding Trust, Privacy and Financial Fears in Online Payment," in 17th IEEE InternationalConference On Trust, Security And Privacy In Computing And Communications, 2018.

[20]"Trends in e-commerce & digital fraud: Mitigating the risks," EKN, 2017.

[21]NikAlifAmriNikHashimet. al, "Internet Shopping: How the Consumer Purchase Behaviour is Impacted by Risk Perception", Test Engineering and Management, Published by: The Mattingley Publishing Co., Inc., Volume 59 Issue 6s Page Number: 1014- 1021, 2019.