International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-3, May 2020
https://doi.org/10.21276/ijircst.2020.8.4.3
www.ijircst.org

An Enriched Information Security Framework from Various Attacks in the IoT

Mohammad Salman Husain, Dr. Mohammad Haroon

ABSTRACT- Security in various E-commerce Applications includes an efficient framework in Information Security especially in Computer Security, Data Security and other online transactions in E-commerce applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from various attacks but Data Storage during the transactions and Computational time of the algorithms is also important. The existing architecture proposed for the security of online e-transactions in web applications provides security from different attacks and is efficient in terms of computational parameters, but there are certain issues which need to be overcome such as: Security Prevention from different attacks during Online Transactions in Web Mining especially in E-commerce Applications, Increase use of Computational Cost at the Client and Server Side. The Proposed framework provides Security prevention from various attacks especially in IoT. The methodology implemented here works on the basis of authenticating the validity of the User by allocating a challenge value and hope that our proposed framework will be more effective and efficient.

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

I. INTRODUCTION

The measures document two workers to produce a common, cryptographically robust important beached on an innovative, low-entropy, communal subversive (i.e., a watchword). The determination in this backdrop is to avert offline terminology occurrences where an adversary

Manuscript received 12 July, 2020.

Mohammad Salman Husain, PG Scholar, Department of Computer Sc. & Engineering, Integral University, Lucknow-India, (salmank094@gmail.com)

Dr. Mohammad Haroon, Associate Professor, Department of Computer Sc. & Engineering, Integral University, Lucknow India

systematically records probable keywords on its particular, undertaking to struggle the precise keyword to perceived etiquette employments. Coarsely, a PAKE technique is endangered if off-line sessions are of no practice and the unsurpassed measure is an online language dose somewhere an opponent necessity dynamically tries to reproduce an authentic gathering using each imaginable watchword. On-line doses of this category are distinguishing in the traditional of password-based authorization; more exceedingly, they can be identified by the waitperson as botched login efforts and fortified alongside. Procedures for reliable key disagreement license two festivities to harvest a mutual, cryptographically durable significant while cooperating over a self-doubting arrangement underneath the inclusive controller of a contestant [20]. Such etiquettes are between the most approximately used and indispensable cryptographic primitives; positively, procedure on a common important is desirable beforehand developed smooth responsibilities such as encoding and communication verification developed conceivable. PAKE measures document two workforces to harvest a shared, cryptographically robust key originated on an innovative, low-entropy, communal underground (i.e., a watchword). Unevenly, a PAKE method is endangered if off streak amounts are of no usage and the greatest incidence is an online vocabulary bout where an enemy must belligerently attempt to mimic an authentic gathering using each conceivable watchword. Online doses of this lesson are inherent in the standard of watchword founded authorization; more conspicuously, they can be distinguished by the waitperson as unsuccessful login exertions and fenced alongside [21]. Maximum watchword grounded user corroboration organizations residence whole belief on the verification waitperson where keywords or effortlessly resultant watchword confirmation statistics are stowed in a dominant folder [3, 19]. Traditional procedures for watchword grounded confirmation undertake a solitary waitron which supplies the entire evidence (e.g., the watchword) essential to confirm an operator. Watchword grounded corroboration is the maximum normally used object confirmation method, owing to the circumstance that no protected stowage is compulsory, and a operator solitary requirements to remember his watchword and then can authenticate wherever, anytime. Maximum of the prevailing watchword based proof arrangements commence the solitary

waitron standard wherever a solitary waitperson transpires in a society. The topmost badly-behaved of the solitary waitron conventional is that the attendant may moment in a solitary fact of devastation, in the wisdom that conciliation of the waitron exposures all manipulator watchwords apprehended by the waitron. Some normally used practices for watchword confirmation are conversed beneath [2, 5]:

A. Two Servers Password Authentication

Two server confirmation instruments are painstaking to be protected for confirming a user in Internet grounded atmosphere. As the quantity of amenities delivered operational is day by day snowballing, operators proposing to use numerous operational amenities are also cumulative. Finished each provision demanding the operator to greatest independently, the upstairs of remembering many employer (Uniqueness) ID /watchword pairs has led to the problematic of unforgettable. In this daily, planned a two-server password authentic key arrangement instrument using watchword where the employer wants to identify his clandestine key. The real-world two waitron watchword verification and key exchange organization that is protected in contradiction of disconnected glossary doses by waitrons once they are skillful by challengers [8, 10].

B. Quantum Channel for two Server Password Authentication

In significant cryptography, significant key circulation etiquettes employment dramatic instrument to allocate meeting answers and community deliberations to checkered for listeners and authenticate the accuracy of a conference significant. Though, communal deliberations necessitate additional communiqué circles among a dispatcher and earpiece and charge valuable quantum bits. The significant based two server keyword authentication procedure flow draw inaccessible and elucidates our construction of two server keyword scheme positioned using the quantum key classical to efficiently store user password in the internet applications. The greatest specimen of this two influence confirmation organization is our present ATM organization, in where the ATM valentine is one influence and the PIN quantity is additional influence. So if the ATM pass is misplaced wages, the validation functionality will be incapacitated. As distant as biometrics is worried, the refuge is self-same active and effectual in this organization ever the less the individual worries are the charge of hardware and software complexity.The waitron is bargained by incomes of a disconnected vocabulary spell. In fresh centuries, abundant courtesy has absorbed on conniving watchword based authentic crucial conversation procedures which can struggle any nice of interloper's dose. To crack this problematic, a new-fangled sympathetic of confirmation assembly baptized the numerous waitperson confirmations was planned. In these numerous server confirmation surroundings, the two-server confirmation etiquette [1] [4] is the humble stand the most satisfactory to users.

C. Two Server Systems

The notion of a manipulator id and watchword is a charge actual and well-organized technique. Recognizing and permitting the sanctioned operator to admittance the possessions is unique of the important characteristics of confirmation organization [7]. A solitary waitron organization is an organization in which the watchword will be kept in a lone waitron. Though seeing the confirmation organization grounded on a solitary waitron, nearby are approximately problems. The solitary waitron organization is susceptible to all categories of bouts from interlopers. The impostor can drudge the organization by tiresome all conceivable explanations till the organization gets cooperated is the maximum positive in the unsociable waitperson arrangement and thorough exploration also can be positive as publicized in Fig 1.

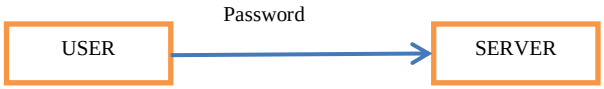

Fig 1: Block Diagram of a Single Server System

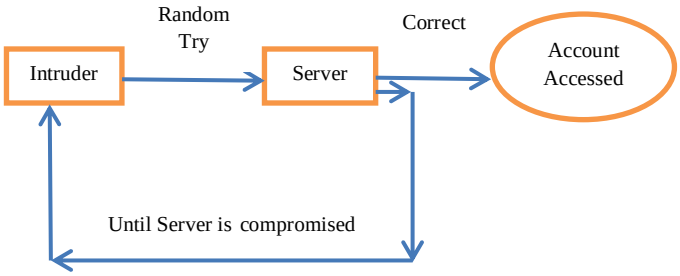

Fig 2: Example of single server system hacked by Intruder

Consequently, it's essential to familiarize the notion of two waitron confirmation organization. In the circumstance of a solitary waitron organization, the attackers can effortlessly negotiation. Nevertheless in the two waitron organization it would not be simply bargained by the aggressor.

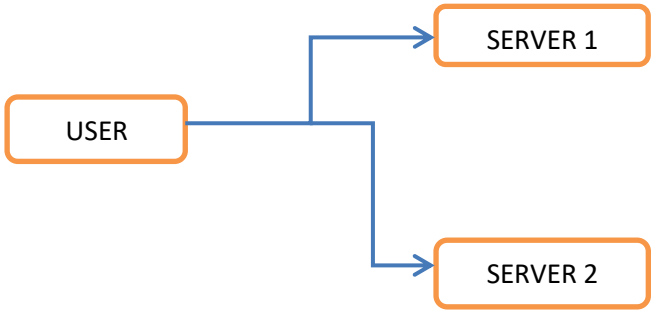

Fig 3: Block Diagram of Two Server System

II. LITERATURE REVIEW

Let's discuss works proposed by various researchers by S. Bellovin and M. Merritt gives the first fruitful password-authenticated key arrangement means were Encrypted Key Exchange means described. Although numerous of the first approaches were defective, the enduring and greater forms of EKE efficiently increase a shared keyword into a collective key, which can be used for encryption and/or message verification. Procedures for genuine key exchange permit two gatherings to produce a communal, cryptographically sturdy key while collaborating over an uncertain network below the comprehensive Regulator of an opponent. Such procedures are amongst the most extensively used and important cryptographic primitives; indeed, arrangement on a common key is essential before higher-level errands such as encoding and memorandum corroboration developed imaginable. Watch word grounded authentic important conversation measures document two operators to harvest a mutual, cryptographically-strong key originated on an original, low-entropy, common underground (i.e., a watchword). Katz, Ostrovsky, and Yung (KOY) [6] established the chief well-organized PAKE procedure with a resistant of refuge in the normal perfect. The technique was unconventional anxious by Gennaro and Lindell (GL), who contributed an overall outline that incorporates the innovative KOY procedure as a singular circumstance. These procedures are protected smooth underneath harmonized presentations by the similar get-together, but necessitate a shared orientation thread. Though this might be fewer attractive than the unadorned classical, dependence on a CRS prepares not seem to be a thoughtful disadvantage in repetition for the disposition of PAKE, where mutual strictures can be hard oblique into an application of the etiquette. The KOY/GL outline necessitates a CCA protected encoding arrangement (such as Cramer-Shoup cryptosystem with a connected straight projective hash connotation and its postponements necessitate four rounds in command to achieve common confirmation. Virtually all succeeding effort on well-organized PAKE in the normal prototypical can be watched as spreading and construction on the KOY/GL outline. Wanga, Z. Cao, K.-K. Choo, and L. Wangthe[9] first proper refuge classical for authentic key exchange conventions between two festivities. The latter has been extended to the password-based setting with security analyses of the above 2-party password-based key exchange, under idealized assumptions, such as the random oracle and the ideal cipher models. Password-based arrangements, provably protected in the normal classical, have been recently proposed but only for two parties. papers considered password-based protocols in the 3-party setting, but none of their schemes enjoys provable security. In fact, our general edifice appears to be the first provably-secure 3-party password-based authentic key exchange etiquette.

D. XiaoFei and M. Chuan Gui[11] introduce additional connected line of investigation is authenticated key conversation in the 3-party location. The primary exertion in this extent is the etiquette of Needham and Schroeder which stimulated the Kerberos disseminated organization. Later, Bellare and Rog away familiarized a prescribed refuge classical in this situation length ways with an edifice of the primary provably protected symmetric crucial grounded key circulation arrangement. In this weekly, we reflect the unusual but vital case in which the underground explanations are pinched from a unimportant set of ethics. Yang et al.'s [16] pointed out about arrangement is susceptible to important cooperation occurrence. Astonishingly, we originate Yang et al.'s arrangement still cannot accomplish its demanded foremost refuge goalmouth by representative a disconnected watchword predicting occurrence in Supplement A, and finished the refuge examination of Yang et al.'s arrangement, some refinements and contests in conniving this type of arrangements, dissimilar from the outdated watchword grounded confirmation, are exposed. Notwithstanding of this, Yang et al.'s prescribed adversary traditional does incarceration the scrupulous two influence corroboration of shrewd card-based keyword authorization preparations: only with both the clever card and the accurate keyword can a user communicate out the smart-card-based keyword authorization procedure absolutely with the isolated corroboration waitron. Xu, J., Zhu, W., Feng, D.[17] planned a general edifice agenda to adapt the conservative provably protected PAKE procedures to shrewd card-based forms and additional intentional an innovative arrangement to validate its efficacy. The new structure is demanded to be locked and can gratify all their projected principles. In the subsequent, we will expression that their outline is essentially disposed to disconnected keyword foreseeing occurrence, thus retreating the power completed that the new structure is protected smooth if the secret statistics packed in smart card is exposed by the opponent. Zubaile Abdullah, Madihah Mohd Saudi and Nor Badrul Anuar proposed a new and efficient technique for the Mobile Botnet Detection using Proof Concept [18]. This tabloid is offering an impermeable of notion on how the bot systems and the continuing exploration to perceive and answer to the movable botnet competently. Discovery of botnet spiteful movement is completed complete an investigation of Cruse wind Botnet cipher using opposite manufacturing development and stationary investigation practice.

III. METHODOLOGY

The Proposed methodology implemented here is based on the concept of authenticating the validity of the User by allocating a challenge value which provides Security prevention from various attacks especially in IoT. The Proposed methodology implemented works on the basis of the following -

- Whenever any new Customer performs any online Transaction on Web, he needs to do handshaking with the Server using shared Challenge value over secure channel. Handshaking between customer and server is done based on challenge value and secrete Shared Password. The Challenge value is limited for a particular Session only.
- After First Factor Authentication, the Customer needs to Register on Server and authenticate using Second Factor Authentication. This phase contains various Steps such as Login / Register / Verification / Password Change.

A. First Factor Authentication using Challenge Handshaking

If in Online Transaction Client want to communicate with Server, then first client sends a request to the server, the server responds. The server asks for the client to enter a challenge value. The server in respond to challenge value generates a master key using MD-5 hashing technique and responds client to enter his unique password. Since every client has its own password, so client enters his password and with the challenge value and password client calculates a master solution and respond back to the server. The server verifies both keys and authenticate client.

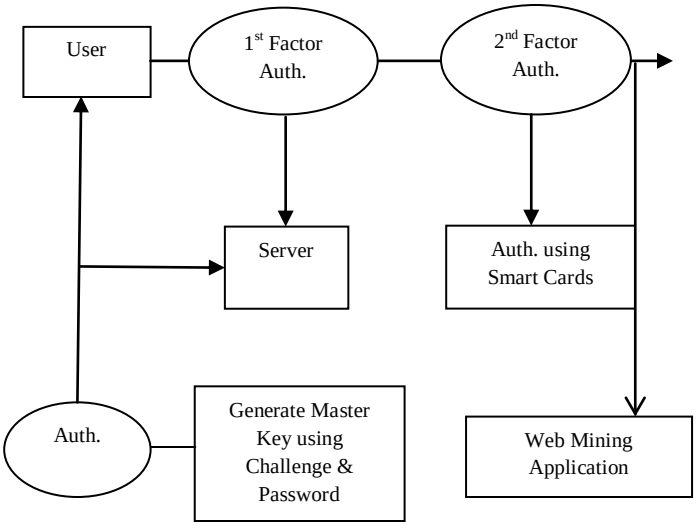

Fig 4 : A framework of Proposed methodology

Algorithm 1

1. First of all Customer will Sends request to the Server for the computed Challenge Value.
2. The Web Transaction Server will take the Challenge Value.
3. Server Computes Time Stamp T1.
4. Server will now take the Password value.
5. Server Sends Challenge Value with Time Stamp T1 to the Customer.
6. Customer then receivers the Challenge Value with Time Stamp T1 from the Server.
7. Customer then Computes Current Time Stamp T2.
8. On the basis of these Time Stamps T1 & T2, Customer calculates total transmission time.

$$Total_{transmission\ time} = 2 * (T2 - T1) + processing\ time$$

9. Customer now takes password and determine MD5 hashing function on challenge value + password +total transmission time.
10. Customer computes MD5 hashing on this data.
11. Customer will sends this data to Server.
12. Server received the data D1 from Customer and computes timestamp T3.
13. Server determines (challenge value + password + T3).
14. Server also determines MD5 hashing on (challenge value + password + T3).
15. If it matches then session is valid. Cheek whether the password valid or not
16. If valid send allowed else send not allowed else session expires.
17. Customer will show whether session expires or not.
18. If not expired then whether password valid or not.

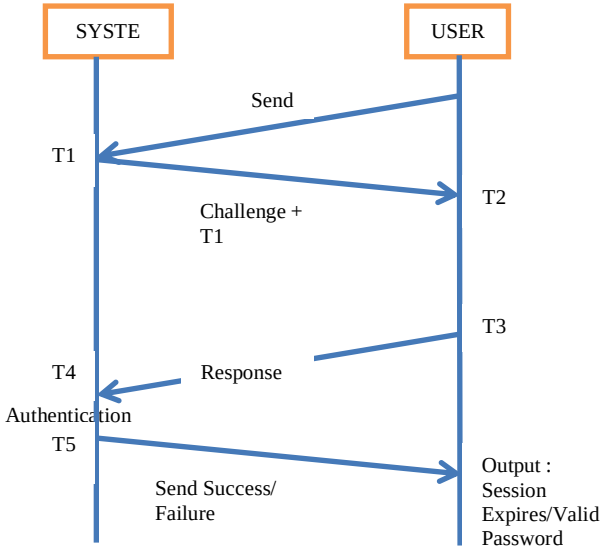

Fig 5: Architecture of the First Factor Authentication using Challenge Handshaking

B. Second Factor Authentication using Improved Smart Cards

The Second factor authentication involves use of Smart Cards for only one time Registration on the Server and Sending and receiving Transaction with high level Security with Asymmetric based Encryption.

The various Annotations used in the algorithms are as follows:

International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-3, May 2020
https://doi.org/10.21276/ijircst.2020.8.4.3
www.ijircst.org

Table 1: Various Annotations used in Algorithm

Customer / Client	U_i
Server	S
Customer ID	ID_i
Customer Password	PW_i
Hash(.)	One Way Hash function such as MD-5 / SHA-1 / SHA-256
$\|\|$	Concatenation
Xor	Xor operation
X	Secrete key of Server S
Tu	Transmission time
ΔT	Difference in transmission time

C. New Client Registration Segment

In the registering segment, client Ui requirements to record in inaccessible server S. Primarily client indicates his/her IDi and PWi. Previously catalogue on Server, recording consultant calculates hash (IDi) and hash (IDi||PWi) and guides to inaccessible server S over a secure frequency. The computed values are encrypted using characteristic based Encoding with Elliptical Curve based solution production and send to Server. Upon reception the registering claims from User Ui. Server Decrypts the Data using his Public Key and verifies the message. Server S analyzes same criticisms associated to the User Ui. 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 stowed a quantity in the elegant tag recollection and subjects this elegant certificate to Client Ui. This smart certificate is transported to Client Ui during a protected network.

a. Authentic Client Login Segment

This segment generates the capability of a protected entering to the client .client requirements to admission same services on distant server S. first it improvement the admittance correct on the isolated server S. Client Ui enters his smart certificate and enters his IDi* and PWi*. The reader calculates –

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

And PCi* = hash (PAi*) and confirms whether PCi (which is generated in the elegant card reminiscence) and PCi* are comparable. If not, dismiss to over repetitive process. or else yes, Client Ui is a genuine possessor of the tidy certificate. On the other hand tag generates an arbitrary nonce Ri and calculates –

$$PE_i = PA_i^*.xor.PR_i$$
$$PC_{id} = hash(ID||PW).xor.PR_i$$
$$PF_i = hash(PA_i||PD_i||PR_i||T_u)$$

Where Tu is existing occasion when client entering request continue and propel the login demand knead {PFi, PEi, PCid, Tu, hash (IDi)} to inaccessible server S.

b. Confirmation/substantiation segment

Upon receiving the login application announcement {PFi, PEi, PCid, Tu, hash (IDi)}. Server authenticates the authority of time impediment between current (Tu') and previous time. Where Tu' is the journey period of the message/data. Current time (Tu')-previoud time (Tu) ≤ difference time (ΔT) where ΔT notates expect convincing time distance for communication impediment. Then server takes the entered appeal and go to subsequently progression, or else the server discard entered appeal.

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 to check PF and PF* are comparable. If not comparable then decline the entered appeal. If identical, then server S calculates–

PFs = hash (hash (IDi) || PDi || PRi || Ts) somewhere, current (Ts time) is isolated server in progress instance and throw recognize message {PFs, G, Ts} to user Ui. Upon receiving concede message smart card calculates

$$G^* = hash(ID_i||PW_i)$$
$$PF_s^* = hash(hash(ID_i)||PD_i||PR_i||T_s)$$

verifies that parameter (G) =G*and PFs = PFs* are identical or not with reciprocated substantiation progression. Here both Server and Client authenticate to each further. If they are identical then tag makes conference solution (Sk) and both Server and Client contribute to it.

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

Otherwise dismiss to over entering progression.

c. Secret code modifies Phase

This stage is concerned every time Client U needs to modify the password (PW) with some more sophisticated Password (PWnew). Client U then enters his generated smart card and enters new (ID*) and new (PW*) and appeal to modify secret word. The tag then verifies parameter (C) = C* are comparable. If it is correct then Client U is a genuine owner of the tag. On the other hand tag asks the Client Ui to participate new code word PWnew. After inward bound the new secret word the tag calculate-

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

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

modify parameter (B) with Bnew and D with Dnew in smart tag memory.

IV. CONCLUSION

Security in various E-commerce Applications includes an efficient framework in Information Security especially in Data and Computer security and other IoT applications. Security in E-Commerce application plays an important role for the secure and scalable transaction which includes various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc. Hence for the Security of Online Transactions in E-Commerce based application various Security algorithms are implemented. Although these Security algorithms are efficient and provides Security from attacks but Data Storage during the transactions and Computational time of the algorithms is also imperative. Hence an efficient algorithm is implemented which provides Security in Online E-Commerce transactions and also provides efficient Computational Cost and time.

The planned procedure implemented here works on the framework of Authentication on Two Factor which provides Security from attacks especially in IoT. The Methodology implemented works on two phases – in first phase assigning the validity of the User by allocating a challenge value and in second phase using improved smart card based authentication. The proposed technique prevents from numerous types of security attacks such as replay attack and identity disclosure attack or outsider attack and provides security from various dimensions such as security-integrity, Confidentiality, Non-repudiation, Privacy etc.

REFERENCES

[1] Xun Yi,"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] Haya Alshehri, Farid Meziane, "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 Moon Lahiri, "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] Shuo Zhai,"Design and implementation of password-based identity authentication system", 2010 International Conference Computer Application and System Modeling (ICCASM), 2010.

[8] Harold Nguegang Tewamba, Jean Robert Kala Kamdjoug, Georges Bell Bitjoka, Samuel Fosso Wamba, Nicolas Nkondock Mi Bahanag, "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] Puspa Indahati Sandhyaduhita, "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] Somdech Rungsrisawat, Thanaporn Sriyakul, Kittisak Jermsittiparsert, "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] Somdech Rungsrisawat, Watcharin Joemsittiprasert, 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, Madihah Mohd Saudi and Nor Badrul Anuar, "Mobile Botnet Detection: Proof of Concept", 2014 IEEE 5th Control and System Graduate Research Colloquium, 2014.

[19] Ghada El Haddad, Esma Aimeur, Hicham Hage, "Understanding Trust, Privacy and Financial Fears in Online Payment," in 17th IEEE International

Conference On Trust, Security And Privacy In Computing And Communications, 2018.

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

[21] Nik Alif Amri Nik Hashim et. 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.

