Biometric Encryption: E-Commerce Security Using Cryptography Techniques

A.D.N.M. Fernando, H.M.P.M.B. Herath, M.L.R.K. Senarathne, D.P. Brandiwatta, T. Kiroshan, M.P. Madushika, P.A.D.A. Senarathne, Mr. Dhishan Dharmmearatchi.

Sri Lanka Institute of Information Technology (Pvt.) Ltd

***Abstract*—** For most businesses stepping into Electronic commerce (E-commerce) is a great advantage. It helps them to improve on supply chain operations, step into new markets, improved customer services, easy operations with suppliers as well as with customers. As a business when they step into Ecommerce they need to protect their online transaction securely with privacy safeness and trusting issues that comes up with different type of intruders. Implementing E-commerce gives these kind of benefits. May be impossible without a coherent, consistent approach to E-commerce security. E-commerce always does its transaction between customers using the internet. For the reason that of these the business should have a high-end security system and should have a good privacy control system. Throughout this paper, will be giving an explanation about the importance of E-commerce security, different type of protocols, public key infrastructures(PKI), digital signature and certificate based cryptography using biometric cryptography and using other techniques that are in cryptography and respectively that supports with the e-commerce security. Using the finger print information the public keys and the private keys will be generated using those information to have a good privacy and confidentiality for the users who will be using this to make transactions in E-commerce more securely. Also as another issue in e-commerce it allows only single transaction at a time for different issues like these they have used different type of techniques.

***Index Terms*—** E-commerce security, High-end security system, Public Key Infrastructure (PKI), Digital Signature and Certificate, Biometric cryptography, Cryptography, Biometric information.

I. INTRODUCTION

Web has gotten to be to a more noteworthy degree, if an unlawful people can access to this system. Idea to ensure system and information transmission over remote system called Network Security and Cryptography. A system security framework ordinarily depends on layers of insurance and fronts of numerous parts including organizing observing and security programming moreover to equipment and machines. All segments work commonly to amplify the taken in general security of the PC system. Cryptography is the security of information should be possible by a procedure. Cryptography is a developing innovation, which is vital for system security.

Electronic business is obtaining and offering of administrations and advantages utilizing through the web or online informal organizations. Electronic business separate on advances, for example, portable trade, store network administration, electronic assets exchange, web showcasing, online exchange handling, electronic information exchange, stock administration frameworks, and robotized information gathering frameworks. Neural system and cryptography together can make an extraordinary help in field of systems security [1].

System security is related in associations, ventures, and different sorts of foundations it can be private, as an organization, and others which may be interested in free. The arrangements and strategies are comprises in network security. It conceals a different PC systems, both open and private, that are utilized as a part of ordinary employments directing exchanges and interchanges between organizations, government offices and people.

An appearance of cryptography in which key used to scramble a message unique in relation to the key used to decode it. Out in the open key cryptography has pair of cryptographic keys named open key and private key, a message can be scrambled with the general population key and decoded with the private key to give security. A message can be scrambled with the private key and unscrambled with the general population key to give marks. Open key has two fundamental branches. There are open key encryption and advanced mark.

When a public key is received over an untrusted channel the recipient often wishes to authenticate the Public key. Finger prints can help accomplish this, since their small size allows them to be passes over trusted channels where the public key won't easily fit.

II. BACKGROUND AND RELATED WORKS

"Review of e-Commerce Security Challenges" authored by Jarnail Singh. Procedure is hash capacity. Preferences in this exploration they demonstrate how security pull in apply in e-trade security and that our E-commerce Server truly never interfaces with the outside world. Burden in this examination paper consider the online fields as it were. Poor security on e-commerce web servers and in clients PCs is center issue to be determined for fast development of E-commerce. Cross-site scripting assaults are an extraordinary instance of code infusion. Web Server Firewall a web server or web application firewall, either an equipment apparatus or programming arrangement, is put in the middle of the customer end point and the web application. The web server and database server ought to be separated from different systems utilizing a system (DMZ) to lessen conceivable interruption from traded off PCs on different systems behind the firewall. In the event that there is a sensible match in the data, the information bundles are then permitted to go into the system which houses our e-Commerce Server [2].

"Design and Development of an E-Commerce Security Using RSA Cryptosystem" authored by J. Nwoye. Procedure is (RSA). Points of interest in this exploration how (RSA) Cryptosystem security draw in apply in security. The security and protection elements of the exchange data are considered as vital variables. People in general key data incorporates n and a subordinate of one of the components of n; an assailant can't decide the prime variables of n (and the private key) from this data alone and that is the thing that makes the (RSA) calculation so secure. RSA cryptosystem is outlined along secluded systems. Doing some electronic trade business on the Internet is as of now a simple undertaking as is tricking and snooping. Open Key Encryption (PKE) or awry encryption is substantially more vital than symmetric encryption for the reasons for e-trade [3].

"Network Security and Cryptography" authored by Mr. R. Kumar, V. Sowmya. Methodology is Rivest-Shamir-Adleman (RSA) algorithm, Digital Signature Algorithm (DSA) and related signature schemes. Advantages in this research cryptographic technology will pay close attention to how public keys are associated with user identities, how stolen keys are detected and revoked and how long a stolen key is useful to a criminal. Disadvantages in this research cryptography cannot understanding of most outside people and the practices of cryptographic security is not available. A general overview of network security and cryptography is provided and various algorithms are discussed. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization. The common technique for masking contents is encryption. Secure Socket Layer (SSL) is most commonly used for securing website transactions. To provide security, the Internet Architecture Board (IAB) included authentication and encryption as necessary security features in the next-generation Internet Protocol (IP), which has been issued as IPv6 [4].

"A Study on E-Commerce Security Issues and Solutions" authored by Pritikana Sen, Rustam Ali Ahmed, Md. Ruhul Islam. Technique is hash capacity. Favorable circumstances in this examination turning the ordinary business to hundred percent EBusinesses and the information don't get lost while transmission and extortion exchange couldn't occur. Inconvenience in this examination online exchange has no security. Secure Socket Layer (SSL) is generally utilized on the Internet, particularly for communication that includes trading secret data. On the off chance that check the site address, by checking the location bar which contains the Uniform asset locator the system can judge whether it is managing right organization or not. Furthermore in the event that will be need to purchase something from this sort of organization the team ought to begin with less costly thing and in a while will get to whether the shopping site is solid or not. Can see whether the shipper plans to impart data to an outsider or subsidiary organization. Brilliant Card Smart card is the card where client individual/business related data is put away and it varies from the Credit Card and check card [5].

"Network Security Issues in e-Commerce" authored by Raghav Gautam, Sukhwinder Singh. Strategy is Distributed Denial of Service (DDOS). Advantages in this exploration online customers inclined to making fledgling blunders. Detriments in this exploration paper leave individuals helpless incorporate shopping on sites that aren't secure, giving out an excessive amount of individual data, and leaving PCs open to infections. Data security is a fundamental administration and specialized necessity for any proficient and successful Payment exchange exercises over the web. E-trade security has its own specific subtleties and is one of the most astounding obvious security parts that influence the end client through their everyday installment connection with business. In the paper the team talks about E-business Security Issues, Security measures, Digital Etrade cycle/Online Shopping, Security Threats and rules for protected and secure internet shopping through shopping sites. Teaching the buyer on security issues is still in the earliest stages organize yet will turn out to be the most basic component of the e-business security design. Ecommerce security is the assurance of e-trade resources from unapproved access, use, adjustment, or decimation [6].

"The study of E-Commerce Security Issues and Solutions" authored by Mr.Amit N. Chaudhari, Prof. Priya V. Shirbhate. Philosophy is Distributed Denial of Service (DDOS). Points of interest in this exploration online customers inclined to making beginner blunders. Weaknesses in this examination paper leave individuals helpless incorporate shopping on sites that aren't secure, giving out an excessive amount of individual data, and leaving PCs open to infections. E-trade Security is a part of the Information Security system and is particularly connected to the segments that influence e-business that incorporate Computer Security, Data security and other more extensive domains of the Information Security structure. E-business security has its own specific subtleties and is one of the most astounding obvious security. In the workshop the team talked about E-trade Security Issues, Security measures, Digital E-business cycle/Online Shopping, Security Threats and rules for sheltered and secure web shopping through shopping sites. E-Commerce security has its own specific subtleties and is one of the most noteworthy obvious security parts that influence the end client through their everyday installment association with business. E-business security is the insurance of e-trade resources from unapproved access, use, modification, or annihilation [7].

Cryptography Based E-Commerce Security, Ritu, 2016, the remote sensor systems develop and turn out to be broadly utilized as a part of numerous applications. E-trade Security is crucial to the system. In this exploration paper clarify the significant security errand of organizations and clients, and portrays the cryptographic systems used to lessen, for example, dangers, clarify the significance of E-trade security and will talk about really great protection, secure E-business convention, open key foundation, computerized mark and testament based cryptography strategies in E-business security. At the point when information goes through numerous hands, data could be caught, encryption plan keeps the information in a good for nothing structure, unless the wafer has the private key [8].

Open key cryptosystem and a key trade /convention utilizing instruments of non-abelian bunch H. K. Pathak, Manju Sanghi, 2008. This examination proposed another open key cryptosystem and key trade convention taking into account the speculation of discrete logarithm issue utilizing Non-abelian gathering of square upper triangular frameworks of higher request. Proposed another open key cryptosystem and a Key of substantial size without the need of huge primes. The security of both the frameworks trusts on the trouble of discrete logarithms over limited fields. Animal power assaults are infeasible if adequately substantial sizes of lattices M1 and M2 are picked. Thus by picking huge qualities for the private keys r, s, v and w man in the center assault can be stayed away from [9].

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems R. L. Rivest, A. Shamir and L. Adlema. This exploration proposed strategy for actualizing an open key cryptosystem whose security reset to a limited extent on the trouble of calculating expansive numbers. In this technique ends up being set up without the utilization of dispatches to convey keys, and it additionally allows one to sign digitized archives. The security of this framework should be analyzed in more detail. Specifically, the trouble of calculating substantial numbers ought to be inspected nearly. Per user is asked to figure out how to break the framework. Once the technique has withstood all assaults for an adequate time span it might be utilized with a sensible measure of certainty. In this paper encryption capacity is the main contender for a trap entryway one way change known not creators. It may be alluring to discover different case, to give elective executions ought to the security of this framework turn out some time or another to be insufficient. There are without a doubt additionally numerous new applications to be found for these capacities [10].

Execution of a Protocol for Secure E-Commerce Transactions Arvind Tudigani, Lahari .D, 2014. This framework we have attempted to give security to E-Commerce exchanges with the blend of symmetric and unbalanced calculations utilized as a part of cryptography. The framework scrambles each message that is being sent to the next remote customer on the system and on the collectors' side decodes the figure content and checks for the privacy of information with hash esteem estimation serving to effectively achieve all the three primitives of system security Authenticity, Confidentiality and Integrity [11].

Research on Digital Signature in Electronic Commerce Hongjie Zhu, Daxing Li, 2008.This paper is to propose a sort of advanced mark in view of open key. Both advanced signature and shielding unlawful insertion and replication of computerized items are adequately figured it out. At last, a material computerized signature framework is given with Java. The primary point of the content is to apply computerized signature innovation in e-commerce framework, propel the answer for the security issues of advanced mark innovation in E-Commerce and offer personality affirmation to the individuals who partake in E-commerce exercises, which keeps a wide range of potential wellbeing dangers. This paper just discuss advanced mark innovation without security of people in general key, and the wellbeing of the general population key will be examined in future [12].

III. CERTIFICATE

Validations tie identity, power, open key, and the other information to a customer. For most web E-trade application, verification using a plan described as a piece of worldwide telecom union telecom systematization region International Telecommunication Union (ITU-T). Suggestion X.509 is utilized. A X.509 authentication contains such data as the:

1- Certificate holder's name and identifier.
2- Certificate holder's open key data.
3- Key utilization limit definition.
4- Certificate strategy data.
5- Certificate backer's name and identifier. 6- Certificate Validity period.

In today's E-trade environment, buyers may get singular affirmations to show their character to a site in the meantime it is the dealer areas that genuinely need assertions to exhibit their character to buyers [13].

IV. E-COMMERCE TRANSACTION SECURITY

In ecommerce exchanges the security must be exhaustive to secure data of the individual in the exchange. Their faculty data must be secured utilizing an open key encryption by giving a Pretty Good Privacy (PGP).

PGP gives a mystery and affirmation organization that can be used for electronic mail and report stockpiling applications. PGP has turned out to be viciously and is at present extensively used, three standard reasons can be alluded to for this improvement: First: It is engaged around count that has survived expansive open review and are considered significantly secure.

Second: It has a broad assortment of propriety.

Third: It was not made by, nor is it controlled by, any managerial or benchmarks affiliation.

PGP is the aftereffect of Phil Zimermann endeavors. It gives a safe correspondence in an unsecured Electronic environment. PGP gives confirmation and classification, pressure and division administrations for e-business exchange Security gave utilizing cryptographic methods. PGP gives a classification and verification benefit that can be utilized for exchanges and document stockpiling applications. It is generally utilized for these sort of a security.

V. PUBLIC KEY CRYPTOGRAPHIC SYSTEM

Using a body part as an input for an e-commerce transaction it is more secured than using number as the security method to secure these transactions. Using the input it generates an optical information signals impressed with the characteristics of a body part; this public key cryptographic system wherein said key generating means compromises to generate a seed number from inverse transform representation and pseudo-random number generator responsive to the seed number generator and a key and then for storing filter information on a data carrier which contains an image of a body part; image based generated seed number. Which will be used as the public keys and the private keys.

a. Authentication

On sender side Secure Hash Algorithm (SHA) -1 is utilized to produce a 160-bits hash code of the sending message. The hash code is encoded utilizing the sender's private key and the outcome is attached to the message. The beneficiary unscrambles the hash code by sender open key. The recipient creates another hash code for the message and contrasts it and the decoded hash code. On the off chance that both hash codes are same then the message is true.

b. Confidentiality

The sender makes a message that will be transmitted and a 128piece number to be utilized as a session mystery key for the sending message. The message is encoded utilizing 3Data Encryption Standard (DES) with the session mystery key. The session mystery key is again encoded utilizing the beneficiary open key and is attached to the sending message. The beneficiary utilized its private key to unscramble and recuperate the session mystery key and after that session mystery key is utilized to decode the sending message.

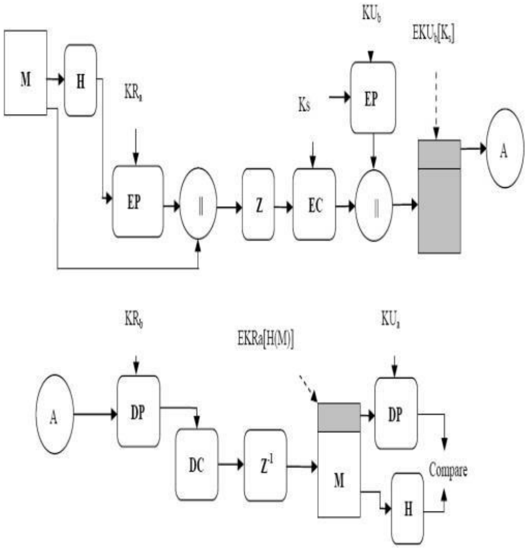


Figure 01: PGP Cryptographic Functions
(Source: https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcTTxy3QN422izddyWPsCT8ILF0Fz5xWrlNRv4K3gJnj4WrWWyNkPw)

Figure 01 portrays the accompanying strides that are performed by PGP to sender side,

i. Hash of Message H (M) is established. ii. Hash is encoded utilizing private key of client A (KRa) and it is linked with message M. iii. At that point Compression (Z) is done utilizing WinZip. iv. After pressure PGP perform symmetric encryption utilizing session key (Ks) and session key likewise encoded utilizing open key of client B (KUb).
v. Toward the end PGP perform link and transmitted to client A

Figure 01 demonstrated the accompanying strides that are performed by PGP to collector side,

i. Unscramble the session key utilizing private key of B (KRb)
ii. At that point utilizing the unscrambled session key recoup the message.
iii. Uncompressed the message (Z-1) and unscramble the message hash utilizing open key of client A (KUa).
iv. Calculate the hash of message and compare with sender's calculated hash value.
v. If both hash are same then message is authentic.

TABLE I
Cryptographic Notations

Notation	Description
M	Message
H	Message Hash
EP, DP	Public Key Encryption & Decryption
EC, DC	Symmetric Encryption &Decryption
Ks	Session Key
KRa, KRb	Private key of user a and b
KUa, KUb	Public Key of user A
Z , Z-1	Compression & uncompressing
||	Concatenation

VI. PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI) gives an establishment to other security administrations. The motivation behind a PKI is to permit the dissemination and utilization of open keys that are created utilizing a biometric data and advanced authentication to give secure correspondence in ecommerce. There are some prevalent open key encryption calculations, for instance, RSA, ElGamal, and ECC. The security of the most open key encryption calculations depends on discrete logarithms in limited gatherings or whole number factorization. A PKI is an establishment on which different applications and system security parts can construct. Frameworks that frequently require PKI based security instruments incorporate Email, different chip card applications, esteem trade with E-business, home saving money, and electronic postal frameworks.

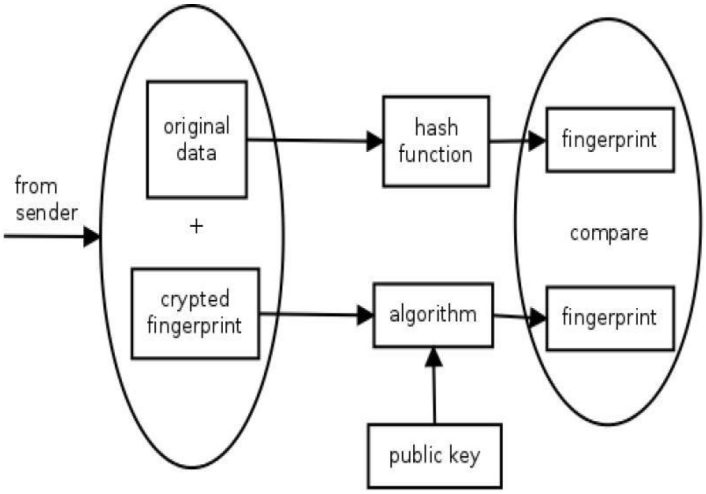


Figure 02: Public Key Infrastructure
(Source: https://www.verboom.net/blog/20130203.0/encryptionsign-2.png)

In above figure 02, sender encodes plain content with his/her private key and connect plaintext with mark. At the point when beneficiary gets then recipient decode it utilizing sender open key. This demonstrates the confirmation utilizing PKI.

The revelation of open key cryptography has made various administrations accessible, some of which were either obscure or unachievable with symmetric figures. One of the primary branches and uses of the general population key cryptography is an open key encryption plan which permits two gatherings to impart safely over an uncertain channel without having earlier learning of each other to build up a mutual mystery key. The procedure utilizes authentications which are issued to clients or applications by a declaration power CA. Issuance of an endorsement requires confirmation of the client's character more often than not by an enlistment power RA. PKI uses digital certificates to protect information assets through the following mechanisms:

i. Verification: Validates the personality of machines and clients.

ii. Encryption: Encodes information to ensure that data can't be seen by unapproved clients or machines.

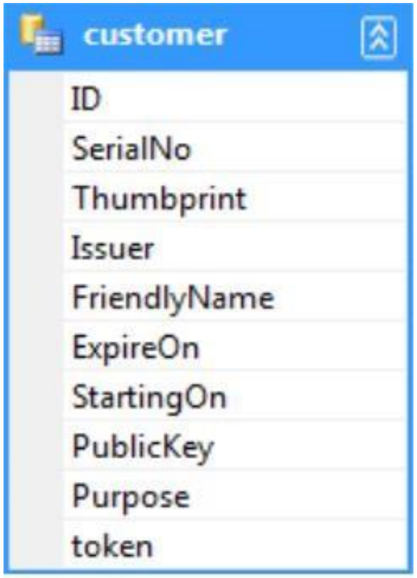
iii. Advanced marking: Provides what might as well be called a biometric signature furthermore empowers ventures to check the honesty of information and figure out if it has been messed with in travel.

iv. Access control: Determines which data a client or application can get to and which operations it can perform once it accesses another application additionally called approval.

VII. SECURE E-COMMERCE PROTOCOL

A Secure E-commerce Protocol gives a testament based security system. In this plan both client and trader demand CIA for issue testaments so both can start their exchange. Both sides will verify each other by their ID's. In this methodology nonce is utilized to handle replay danger. Client and Merchant testaments diagram are appeared in fig 3, 4. The blueprint contains ID, declaration serial number, guarantor name, reason for testament ,endorsement hash code , begin date , lapse date and so forth.

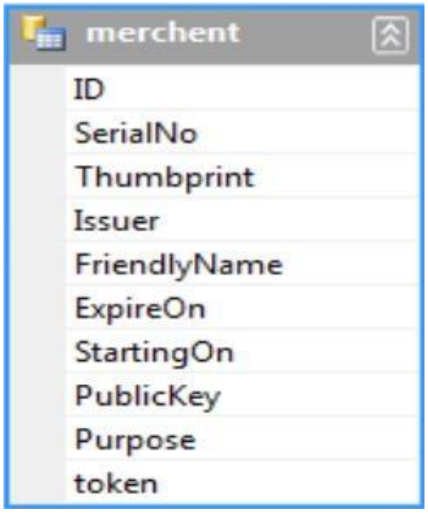
Endorsement is encoded by private key of CIA (EPR (CIA)).



customer

ID
SerialNo
Thumbprint
Issuer
FriendlyName
ExpireOn
StartingOn
PublicKey
Purpose
token

Figure 03: Customer Certificate Schema
(Source: http://ijcsjournal.com/sites/default/files/archives/IJCS-072.pdf)



merchent

ID
SerialNo
Thumbprint
Issuer
FriendlyName
ExpireOn
StartingOn
PublicKey
Purpose
token

Figure 04: Merchant Certificate Schema
(Source: http://ijcsjournal.com/sites/default/files/archives/IJCS072.pdf)

TABLE II
Secure E-commerce Protocol Steps

i.	EKU (Auth) [IDA, ReqA, Time, KUA, NA]
ii.	EKU (Auth) [IDB, Time, KUB, NA]
iii.	CA=EKR (Auth) [IDA, ReqA, Time, NA]
iv.	CB=EKR (Auth) [IDB, Time, KUB, NB]
v.	TA→M
vi.	TB →C
vii.	Eku (B) [N1, EKR (A) [IDA, Time, NA]]
viii.	Eku (A) [N2, EKR (B) [IDB, Time, NB]]
ix.	Eku (B) [EKR (A) [N2]]

Secure E-commerce Protocol provides security against Authentication, Confidentiality, Integrity, Non Repudiation, Replay attack and man in the middle attack [14].

TABLE III
Secure E-commerce Protocol Notations

Notation	**Description**
CIA	Certificate Issue Authority
CA, CB	Certificate issue to user A
N1, N2	Nonce generated by user A
Time	Time Stamp
IDA, IDB	Identity of user A and B
EKR(A), EKR(B), EKU(A), EKU(B)	private/public encryption using private/public . keys of user A and B

VIII. E-COMMERCE SECURITY

There are unmistakable techniques used to ensure and measure security in E-trade environment, ought to clear up some of them in the going with sections, which are: Privacy, Cryptography and statements.

IX. CRYPTOGRAPHY

Cipher systems are ordered into 2 classes which are:-
a. Secret key figure framework.
b. Public-key figure framework

In the going with ought to depict every one class rapidly Discharge Key: Secret key cryptography is the most settled kind of system in which to form things in puzzle. There are two essential kind of release key cryptography, transposition and substitution. Transposition figure, encode the main message by changing characters demand in which they happened. Where as in substitution figure, the principal message was encoded by supplanting there characters with various characters. In both sorts, both the sender and authority have the same puzzle keys. For the most part used puzzle key arrangement today is called Data Encryption Standard (DES). DES figure work with a 56-bit riddle key besides 16 rounds to change a square of plaintext into figure content.

X. FUTURE WORK

With explosive growth in the Internet, network and data security have become an inevitable concern for any organization whose inner private network is connected to the Internet. The security for the data has become highly essential. User’s data privacy is a central problem over cloud. With more mathematical tools, cryptographic schemes are getting more adaptable and often involve multiple keys for a single application.

In the future, work can be prepared on key distribution and management as well as an ideal cryptography techniques for data security over clouds.

XI. CONCLUSION

Satisfying security requirements is the most important goals for e-commerce system security designers. Public key cryptographic techniques are used in the e-commerce transactions. This is more secured than using number as the security method. With the input it generates an optical information signals impressed with the characteristics of a body part. Which will be used as the public keys and the private keys.

In the proposed paper, it has been designed for securing ecommerce transaction by using public key encryption algorithm which is based on discrete logarithms in finite groups or integer factorization. A Public Key Infrastructure (PKI) is a foundation on which other applications and network security can build. System that often required PKI based security mechanisms. The proposed method is increase the performance of E-commerce security rapidly. So combining more security methods with each other may increase efficiency but may increase the cost.

ACKNOWLEDGEMENT

I wish to thank Mr. Dhishan Dharmmearatchi of Sri Lanka Institute of Information Technology (Pvt.) Ltd., Colombo, for the helpful criticism, encouragement, scholarly instruction and suggestions for improvement which he gave me throughout the period of this work.

REFERENCES

[1] S. Kumar, “Technique for Security of Multimedia using Neural Network” [Online]. Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014. [Online]. Available: http://www.ijircce.com/upload/2014/february/1_Review.pdf [Accessed: 7- Sep- 2016].

[2] J. Singh, “Review of e-Commerce Security Challenges”, *International Journal of Innovative Research in Computer and Communication Engineering*, ISSN: 2320-9801 Vol. 2, Issue 2, February 2014. [Online]. Available: http://www.ijircce.com/upload/2014/february/1_Review.pdf [Accessed: 7- Sep- 2016].

[3] J. Nwoye, "Design and Development of an E-Commerce Security Using RSA Cryptosystem", School of Science & Technology, National Open University of Nigeria, Enugu, Nigeria, 2016. [Online]. Available: http://www.ijiris.com/volumes/vol2/iss6/02.JNIS10083.pdf. [Accessed: 14- Sep- 2016].

[4] R. Kumar, V. Sowmya, “Network Security and Cryptography”, International Journal of Computer Science and Information Technology Research ISSN 2348-120X Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014. [Online]. Available: http://www.researchpublish.com/download.php?file=NETWORK%20SECURITY%20AND%20CRYPTOGRAPHY-253.pdf [Accessed: 13- Sep- 2016].

[5] S. Pritikana and R.A. Ahmed “A Study on E-commerce Security Issues and Solutions”, International Journal of Computer and Communication System Engineering (IJCCSE), Vol. 2 (3), 2015, 425-430. [Online] Available: http://www.ijccse.com/june15/RP_0615_5886.pdf [Accessed: 11- Sep- 2016].

[6] R. Gautam, S. Singh, 2014. “Network Security Issues in e-Commerce”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014 ISSN: 2277 128X. [Online] Available: http://www.ijarcsse.com/docs/papers/Volume_4/3_March2014/V4I30104.pdf. [Accessed: 6- Sep- 2016].

[7] M. A. N. Chaudhari, V. Shirbhate, Prof. Priya. “The study of E-Commerce Security Issues and Solutions”, [Online]. Available: http://ijrise.org/asset/archive/15SANKALP4.pdf [Accessed: 6- Sep- 2016].

[8] Mr. Ritu, "Cryptography Based E-Commerce Security", *https://www.ijarcsse.com*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 7, July 2016. [Online]. Available: https://www.ijarcsse.com/docs/papers/Volume_6/7_July2016/V6I70111.pdf. [Accessed: 14- Sep- 2016].

[9] H.K Pathak and S. Manju, “Public key cryptosystem and a key exchange protocol using tools of non-abelian group”, 1st ed. (IJCSE) International Journal on Computer Science and Engineering, 2016, p. 5. [Online] Available: http://www.enggjournals.com/ijcse/doc/IJCSE10-02-04-39.pdf [Accessed: 11- Sep- 2016].

[10] R. L. Rivest, A. Shamir and L. Adlema, "A method for obtaining digital signatures and public-key cryptosystems" (2008). [Online] Available: http://www.cs.sfu.ca/~vaughan/teaching/431.2011/papers/citation.cfm.html. [Accessed: 5- Sep- 2016].

[11] A. Tudigani, A. Lahari, "Implementation of a Protocol for Secure ECommerce Transactions," *International Journal of Computer Science and Mobile Computing*, Vol. 3, no. 7, p. pg.499 – 505, Jul. 2014. [Online] Available: http://www.ijcsmc.com/docs/papers/July2014/V3I7201499a1.pdf [Accessed: 13- Sep- 2016].

[12] H. Zhu and D. Li, “Research on Digital Signature in Electronic Commerce”, Proceedings of the International Multi Conference of Engineers and Computer Scientists, (2008). [Online] Available: http://www.iaeng.org/publication/IMECS2008/IMECS2008_pp807-809.pdf [Accessed: 13- Sep- 2016].

[13] J. Menezes, A. Vanstone, “Handbook of Applied Cryptography”: CRC Press, 1996.

[14] M. A Nada, “E-Commerce Security”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008. [Online].Available: http://paper.ijcsns.org/07_book/200805/20080550.pdf. [Accessed: 11- Sep- 2016].

AUTHORS

First Author – A.D.N.M. Fernando, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology (Pvt) Ltd, Niranjanfernando256@gmail.com.

Second Author – H.M.P.M.B. Herath, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology (Pvt) Ltd, paramee93@gmail.com.

Third Author – M.L.R.K. Senarathna, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, lakchani.senarathna@gamil.com.

Forth Author – D.P. Brandiwatta, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, damithpriyanath@gmail.com.

Fifth Author – T. Kiroshan, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, kiroshan.t@gmail.com.

Sixth Author – M.P. Madushika, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, pavanimadarasinghe@gmail.com.

Seventh Author – P.A.D.A. Senarathne, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, A.senarathna121@gmail.com.

Eighth Author – Dhishan Dhammearatchi, Lecturer(Bsc Hons(UK), MSc (UK), CCNP, MCSSL(SL), MBCS(UK), MIEEE, TM (CC), MCKC (SL)), Sri Lanka Institute of Information Technology(Pvt) Ltd, dhishan.d@sliit.lk.

Correspondence Author – H.M.P.M.B. Herath, paramee93@gmail.com, +94772856045