ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 4, 133-138 (2017)

www.astesj.com

ASTESJ

ISSN: 2415-6698

An Efficient Authentication Method For Smart Card Verification In Online

Kanamarlapudi Venkata Srinivasa Rao[1], Ramanathan Udayakumar[*, 2], Velu Khanaa[3]

[1]*Research Scholar, Department of CSE, BIHER University, Chennai – 73, India*

[2]*Associate Professor, Department of Information Technology, BIHER University, Chennai – 73, India*

[3]*Dean-Info. BIHER University. Chennai-73, India*

ARTICLE INFO

Article history:
Received: 10 July, 2017
Accepted: 02 August, 2017
Online: 20 August, 2017

Keywords:
Zero-data
Encryption
Decryption
Smart card
Authentication
Password

ABSTRACT

The great cards are getting a charge out of a critical part inside the on-line managing wherever we have tendency to can't check the cardholder up close and personal. The phishing sites may parody the data in the middle of the customer website and along these lines the common webpage. To protect the data and managing here we have tendency to are presenting the three level confirmations. In arranged approach there are two stages i.e. Enlistment and login. All through enlistment part control the word which can figure and separated into two segments i.e. parcel one can keep inside the client or customer viewpoint, segment a couple of can keep in server perspective. Next level is to exchange the client icon which can figure and split into two shares each are keep severally. In the end zero information code will be get refreshed and it's furthermore get keep as two components. All through the login part before starting the managing the client and server ought to uncover their three-genuine data offers if each stacked data got coordinate then the client is legitimate and server isn't a phishing site.

1. Introduction

In the on-line managing the secured air is one among the key variables; to create the secured environment here we tend to are proposing three level validations. All through the enlistment section three essential true data are entered by the client. All the primary focuses are acquainted in with the procedure thus split into two offers. [1-2] Each individual share is keep in customer and server viewpoint.

In the enlistment part to attempt and do check on client, uncover a couple of offers from customer and server the client confirms the server for phishing site and server confirm the client verification? The shares keeping up in two databases are scrambled one while not knowing the mystery composing method and share two one can't get the cardboard holder and card information. [3]

The phishing sites can't be identified in conventional managing strategy, however in our philosophy though doing giving one can't enter their card data while not exchanging the correct information inside the customer viewpoint data also server should transfer the enlisted information presently the customer shares and server shares are to be stacked along for acquiring the main genuine data. Presently if the client human movement with phishing site they can't turn out the correct information.

This paper is composed as takes after. Associated take a shot at positive distinguishing proof is checked on in Section-II. In Section-III depicts Existing system, in Section-IV depicts Methodology, in Section-V manages arranged philosophies, in Section-VI Portrays Implementation and Section-VII depicts Conclusion and Future Work.

2. Related Work

Prescribe however current instruments shield against disconnected papers taking assaults, powerful assurance against on-line channel-breaking assaults needs advancements to annihilation man-in-the-center (MITM) assaults, and sensible insurance against substance control assaults needs exchange verification innovations. [4-5]

Arranged a change to Chin subject to thwart from a few shortcomings. Notwithstanding, the enhanced subject isn't exclusively still at danger of parallel session assault, however also unreliable for dynamical the client's assertion in word alteration part. thus, the present paper presents Associate in Nursing change to determine such issues. Accordingly, the arranged subject grants clients to adjust their passwords openly and immovably while not

[*]Corresponding Author: Ramanathan Udayakumar, Department of IT, BIHER, Bharath University, Chennai – 73, India | Email: rsukumar2007@gmail.com

the help of a faraway server, though furthermore giving secure common authentication. [6-8]

Propose an ultra-low memory unique mark coordinating algorithmic govern and execute it on a 32-bit positive recognizable proof. we tend to first be assessed each the amount of bearings raised and memory request of each progression of a commonplace unique mark coordinating algorithmic run the show. At that point, we have a tend to build up a memory-effective algorithmic lead for the principal memory overpowering stride arrangement by doing extra calculations inside the limitation of the day and age request. Our trial comes about demonstrate that the arranged algorithmic manage will decrease the fancied memory house by a component of sixty-two and might be ere cured in day and age on a 32-bit positive recognizable proof. [9-11]

Presents a simple and temperate client verification approach bolstered a firm mouse-operation assignment for each specimen of the mouse-operation assignment, every old all-encompassing choice and recently characterized procedural [12] choices are removed for right and fine-grained portrayal of a client's particular mouse conduct. Separate estimation and Manfred Eigen house-change systems are connected to get include components for with effectiveness speaking to the main mouse highlight space. At that point, a one-class learning algorithmic govern is used inside the separation based component Manfred Eigen house for the validation errand. The approach is assessed on a dataset of five,550 mouse-operation tests from thirty-seven subjects. escalated test comes about are encased to exhibit the effectuality of the arranged approach, that accomplishes a false-acknowledgment rate of 8.74%, a false-dismissal rate of 7.69% with a comparing verification time of 11.8 seconds. Two additional trials are giving to check the present approach [13] with option approaches inside the writing. Our dataset is out in the open offered to encourage future examination.

Propose a totally extraordinary client confirmation and key understanding topic exploitation great cards for multi-server situations with a considerable measure of less process esteem [14] and extra reasonableness. the primary merits include: (1) clients exclusively should enroll at the enlistment focus once and will utilize admissible administrations in qualified servers; (2) the subject doesn't need a check table; (3) clients will unreservedly settle on their passwords; (4) the calculation and correspondence esteem is to a great degree low; (5) servers and clients can confirm each other; (6) it creates a session enter in understanding by the client and in this way the server; (7) it's a nonce-based topic that doesn't have an overwhelming time-synchronization [15] disadvantage.

Propose a solid and sparing client validation and key understanding topic exploitation great cards. the most merits grasp the accompanying: 1) the calculation and correspondence esteem is to a great degree low; 2) there's no need for any word or check table inside the server; 3) a client will openly decide on and modify his own watchword; 4) it's a nonce-based topic that doesn't have an overwhelming time-synchronization issue; 5) servers and clients will prove each other; 6) the server will renounce a lost card and issue a swap card for a client while not dynamical his personality; 7) the security of clients might be ensured; 8) it creates a session scratch indicated by the client and in this way the server; and 9) it will stop the disconnected wordbook assault yet the key information continue amid a constructive ID is bargained. [16-18]

Arranged plans, application servers don't should keep up a confirmation table and this cherished preferred standpoint isn't tended to by past grant. In addition, the protection of clients is moreover tended to in Liao-Wang's subject [19]. amid this article, we tend to demonstrate that their plans don't appear to be secure against the server caricaturing and in this manner the pantomime assaults. At that point, we have a tendency to propose a solid client validation subject to confront up to these assaults and keep consistent merits.

Propose a totally one of a kind trilateral key trade subject exploitation great cards. the most merits of our subject include: (1) there cravings no confirmation, passwords or shared keys table inside the reliable server; (2) clients will openly settle on and adjust their own passwords; (3) the correspondence and calculation esteem is to a great degree low; (4) Two clients will prove each other by the dependable server; (5) it produces a session enter in assertion between two clients; (6) it's a nonce-based topic that doesn't have an overwhelming time synchronization disadvantage.[20-21]

3. Existing System

3.1 *Existing Authorization Procedure:*

When the client starts the dealing, they're sent to secure servers to complete the checkout method. The cardholder places Associate in Nursing order at the merchant's website by clicking the "Send Order" button on the Review Order page throughout checkout. [22-23]

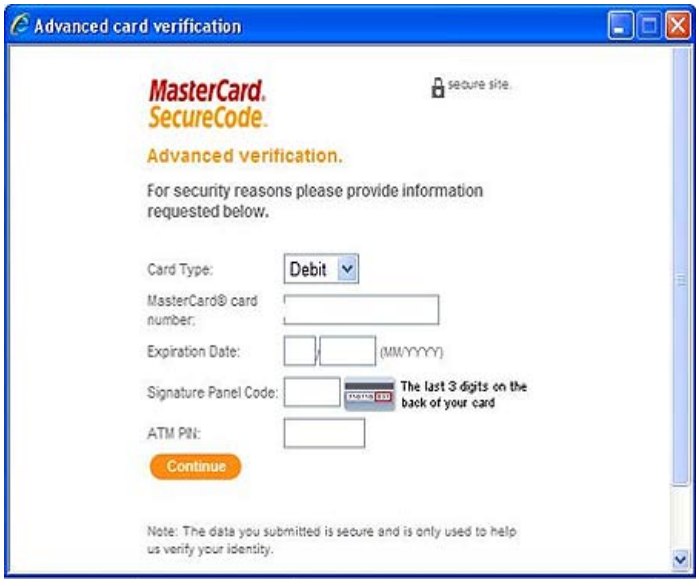

Figure 1 Existing System

(First Data Merchant Services) FDMS sends the authorization request to the issuing bank (or credit card association).

The authorization request includes:

- the credit card number

- expiration date
- the billing address (used for AVS validation)
- the CVV number (if entered)
- the amount of the order

The Issuing Bank (or Credit Card Association):

- validates the card number and expiration
- checks the amount of the order against the available credit
- checks the billing address provided against the billing address on file
- validates the CVV number (if provided)

If approved, the amount of the order is reserved from the total of available credit for the cardholder. [24-26]

The Issuing bank (or Credit Card Association) sends the authorization response to FDMS. The authorization response consists of either an approval along with Address Verification System (AVS) and Card Verification Value (CVV) response codes or a decline. Depending on the state of the authorization, the cardholder receives instructions or confirmation of the order. [27-28]

In the above process, there is no specific authentication process except password which can be easily deceived by the intruders. [29]

4. Proposed Methodology

4.1 Text substitution cipher algorithm Cryptography:

Cryptography is the system where encryption and decryption techniques are used to the network and computer for the security of the data. Encryption means the change of original information (plain text) into another form by some operations (algorithm) and decryption means the techniques of getting the original information by some operations (algorithm) from the encrypted data (cipher text).

During the registration, the user will first enter the Key value and then the password, the entered string of password is introduced into the cryptography algorithm using key value. Then obtained encrypted value is divided into two partitions evenly. First part gets stored in client and second part stored in server.

$$CT = \begin{cases} M = M + C & if\ M = 0 \\ M = M - C & if\ M > 0 \end{cases}$$

Where A=ASCII summation of Key

M=A % 2

CT= Cipher Text

Substitution algorithm

Input: Two values Password and Key value

Output: Stored two partitions, one part in Client and second part in Server.

Step-1: Accept the Password string.

Step-2: Accept the Key value from the user.

Step-3: Compute ASCII summation of Key Value C.

Step-4: For Each character in password string do the following

Step-5: Find the ASCII value of the character.

Step-6: Compute M= ASCII value Mod 2

Step-7: If M==0 then

Encrypted Character = M+C

Else

Encrypted Character = M-C

Step-8: Now repeat Step 4 to step 7 to obtain the cipher text.

Step-9: Cipher Text is introduced for length calculation L.

Step-10: Compute L/2, Part1 = 0 to L/2 and

Part 2 = L/2+1 to L.

Step-11: Individual Parts are stored in client and server respectively.

4.2 Image encryption and sharing procedure

Given Passport size photo is a shared secret image with M×N pixels. The dealer can derive shadows from M×N and generate two shared images. The new sharing process is introduced here. Given images, the secret image can be recovered with no distortion. The cover images could be reconstructed with limited distortion from specific value calculated.

4.3 Sharing procedure

The dealer chooses Odd or Even value combination from the pixel of given image. To share the secret image with the dealer converts given pixel of grayscale image into M×N pixel matrix. For instance, we assume that the chosen number is equal to odd or even and if it is odd then the corresponding pixel position is moved to share-1 and vice versa. The following algorithm illustrates the entire procedure in detail.

4.4 The algorithm

Input: One secret image

Output: Two matrices, One in share-1 and second in share-2

Step1- Take the input image and derive the M X N pixels.

Step2- Convert the given image into grayscale image. Apply the procedure to find the positions $(x_1, y_1), (x_2, y2), \ldots, (x_n, y_n)$ of the image pixels.

Step3- Use the function to calculate the odd or even characteristic of the image pixel position.

Step4- Maintain the two matrices called share-1 and share-2.

Step5- Use step3 and split the odd pixels and even pixels in the manner that, (Odd, Odd), (Odd, Even) in share-1 and (Even, Even) (Even, Odd) in share-2.

Step6- Apply pixel positions in order, for easy retrieval.

Step7- Apply pixel reversal to reverse the obtained pixels, in share-1.

Step8- Store the reversed Pixel in matrix as image called share-1.

Step9- Apply pixel reversal to reverse the obtained pixels in share-2.

Step10- Store Reversed Pixel' 'in matrix as image called share-2.

Step11- Repeat point 1 to 10 for original image (i.e. matrix of original image) to shared images conversion.

4.5 *Zero knowledge authentications*

Zero-data protocols area unit fascinating tool for the authentication verification the two stack holders here area unit Prover and supporter. The prover has got to prove himself victimization queries generated by the supporter. If the prover did not prove himself he's not attested. Zero-data protocol comprises two steps particularly Identification and Operation. Identification schemes area unit strategies by that a prover might prove his or her identity while not revealing data which will be utilized by associate degree listener to impersonate the prover. The operation done by the supporter is to verify the small print entered by the prover. Once the cardboard holder completed registration by coming into the non-public knowledge is distributed to host server. The host server successively verifies the number that is first part of authentication. For second part of authentication zero-data technique is employed.

p → v Prover to Verifier Code Passed

v → p Verifier to Prover authentication set

p → v Update zero knowledge code

5. Proposed System

In our planned system, there are a unit two phases Registration and Login part. throughout the registration part the user ought to enter the three vital authentic data and the data area unit encrypted and split into two components.

5.1 Registration Phase:

In the registration part, the system exploits three totally different authentication data,

i) User Password (with key string)

ii) Passport size image of card holder.

iii) Zero information code to be updated.

Here of these data area unit encrypted and split into two totally different components. every half goes to induce hold on within the consumer and server databases one by one. The secret is encrypted mistreatment substitution cipher formula. [30-31] Then the obtained text is split into two. The image of the user ought to get uploaded within the system. The image is shared mistreatment the formula and so odd and even pixels area unit split into two shares. eventually zero information updated code is additionally split into two components. One part of the all on top of three is get hold on in consumer and another part can get hold on in server information. [32]

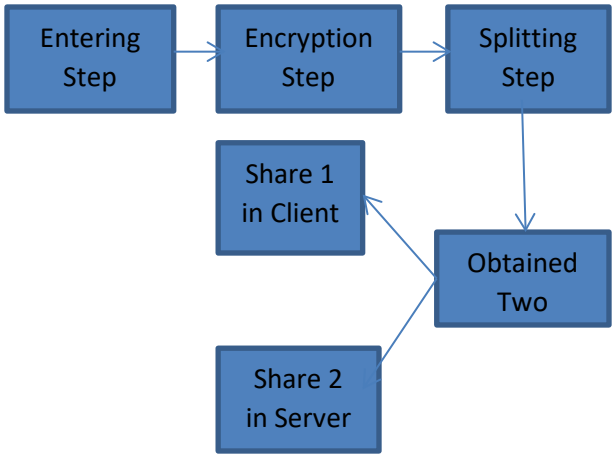

Figure 2 Registration Phase

During the coming into step input the desired details like positive identification text, user image and the zero-data code. Then within the coding step with the various algorithms mentioned higher than given inputs square measure encrypted. Then the encrypted outputs square measure spliced into two halves the two shares square measure get keep in consumer (user) and the server machine.

5.2 Login Phase:

During login section the user have to be compelled to enter Share one details of the positive identification, uploaded image and updated zero-data code, subsequently server reveal its share a pair of each of the shares square measure going stacked along and eventually apply the decipherment rule on positive identification, Image and nil data code then server verifies user positive identification and consumer verifies the image and nil data if each of them proved themselves currently consumer will enter the cardboard info for secured dealing decipherment is often done on the positive identification and image victimization the algorithms explained within the higher than section. [33]

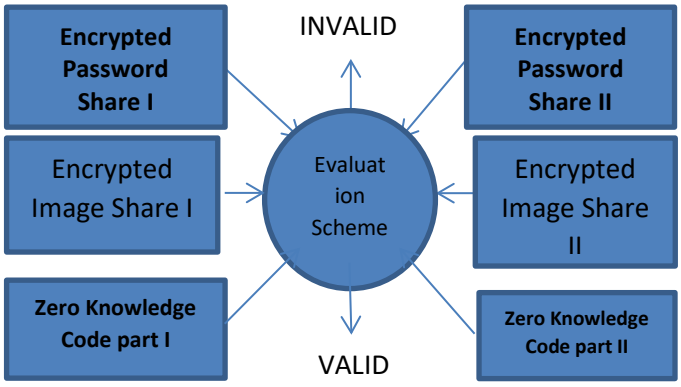

Figure 3 Login and Verification Phase

6. Implementation

In the suggested system first step is registration phase where users must upload three different information level by level. During the first level, the user must enter their password and password key as depicted in the Fig.4.

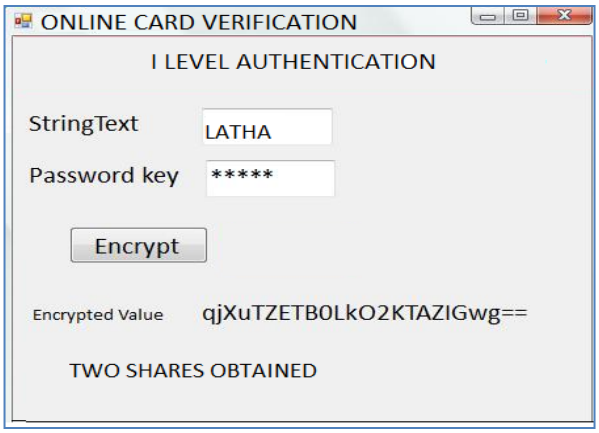

Figure 4 I Level Authentication

In the second level, they must upload their photo. Then the user can get the share that was encrypted using the respective algorithm.

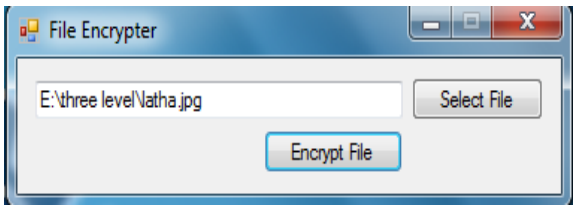

Figure 5 Image Encryption

Finally, the user must enter the zero-knowledge code which can be updated at the end of the transaction. During login phase the process has been reversed.

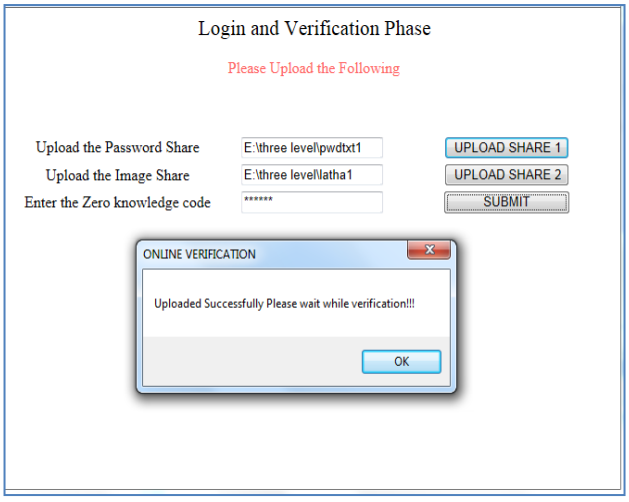

Figure 6 Login and Verification phase

After processing the three inputs the user can either precede to the transaction, else if their identity is not valid then exit from the login and it will not precede the transaction further. The validity of user will be intimated to the server and validity of server will be intimated to user.

7. Conclusion and Future Work

The arranged philosophy jam positive distinguishing proof information of client's exploitation three levels of security. to begin with level checks regardless of whether the cardboard holder could be a legitimate individual or not. On the off chance that the individual isn't substantial he can't enter revise positive recognizable proof and key for cryptography. Second level of validation is to confirm regardless of whether the server could be an honest to goodness/secure site or a phishing site, If the site could be a phishing then in that situation, the phishing site can't demonstrate the picture for that specific client to account of the established truth that the picture is produced by the stacking of two shares, one with the client and furthermore the option with the specific information of the site.

References

[1] Debanjan Das1, Megholova Mukherjee2, Neha Choudhary3, Asoke Nath Joyshree Nath"An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm".

[2] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[3] Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[4] R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.

[5] G.Megala1 A.Rajeswari2 V.Visalatchi3 Mr.B.Ganes "An Improved Secret Image Sharing Scheme with Steganography." 2011 IEEE.

[6] Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.

[7] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm Neeraj Khanna,Sayantan Chakraborty,Joyshree Nath ,A.K.Chaudhuri ,Amlan Chakrabarti ,A.K.Chaudhuri , Asoke Nath 2011 International Conference on Communication Systems and Network Technologies.

[8] Li Lu, Member, IEEE, Jinsong Han, Yunhao Liu, Lei Hu, Jinpeng Huai, Lionel M. Ni, and Jian Ma "Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps" Ieee Transactions on Parallel And Distributed Systems, Vol. 19, No. 10, October 2008.

[9] Ieee Sensors Journal, Vol. 11, No. 12, December 2011 3235 Zero-Knowledge Authentication Protocol Based onAlternative Mode in RFID Systems Hong Liu, and Huansheng Ning.

[10] Wen-Shenq Juang, Sian-Teng Chen, And Horng-Twu Liaw Robust And Efficient Password-Authenticated Key Agreement Using Smart Cards Ieee Transactions On Industrial Electronics, Vol. 55, No. 6, June 2008.

[11] Mrs. Hemangi Kulkarni, Aniket Yadav, Darpan Shah, Pratik Bhandari, Samuya Mahapatra "Unique ID Management" Aniket Yadav, ,Int.J.Computer Technology & Applications,Vol 3 (2), 520-524.

[12] Hamed Taherdoost, Shamsul Sahibuddin & Neda Jalaliyoon "Smart Card Security; Technology and Adoption" International Journal of Security (IJS), Volume (5): Issue (2): 2011.

[13] Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.

[14] Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.

[15] Rui Wang, Shuo Chen, XiaoFeng Wang, Shaz Qadeer "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores" 2011 IEEE Symposium on Security and Privacy.

[16] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.

[17] "R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017."

[18] R. Elankavi, R. Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.

[19] Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.

[20] Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.

[21] Afzel Noor "Highly Robust Biometric Smart card design" IEEE 2000.

[22] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[23] Thomas Ezat A Dubbish, Robert H Slon "Examining the smart card security under the threat of Power analysis attack", IEEE transactions on computer April 2004.

[24] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[25] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo "Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards" IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, MAY 2004.

[26] Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[27] Chao Shen,Zhongmin Cai, Xiaohong Guan, *Fellow,* Youtian Du,and Roy A. axionUser Authentication through Mouse Dynamics" 2011 IEEE.

[28] Wen-Shenq Juang "Efficient Multi-server Password Authenticated Key Agreement Using Smart Cards"Manuscript received January 15, 2004.

[29] Wen-Shenq Juang, Sian-Teng Chen, and Horng-Twu Liaw "Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards" 2008 IEEE.

[30] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[31] Ren-Chiun Wang, Wen-Shenq Juang, and Chin-Laung Lei, *Member, IEEE* "User Authentication Scheme with Privacy-Preservation for Multi-Server Environment" . IEEE COMMUNICATIONS LETTERS, VOL. 13, NO. 2, FEBRUARY 2009.

[32] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[33] Wen-Shenq Jaung Efficient Three-Party Key Exchange Using Smart Cards Contributed Paper Manuscript received April 8, 2004.