Online Smart Card Verification Using Three Level Authentication

Dr.V. Khanna, Dr.R. Udayakumar

Abstract: The smart cards are playing a vital role in the online transaction where we cannot verify the cardholder in person. The phishing websites may spoof the data in between the client site and the merchant site. To protect the data and transaction here we are introducing the three level authentications. In proposed methodology there are two phases i.e. Registration and login. During registration phase manipulate the password which will encrypt and divided into two partitions i.e. partition 1 will stored in the user or client side, partition 2 will stored in server side. Next level is to upload the user photo which will encrypt and split into two shares each are stored separately. At last zero knowledge code will be get updated and it is also get stored as two parts. During the login phase before starting the transaction the user and server must reveal their three authentic information shares if both stacked data got match then the user is valid and server is not a phishing website.

Keywords: Zero Knowledge, Encryption, Decryption, Smart Card, Authentication, Password.

INTRODUCTION

In the online transaction the secured environment is one of the important factors; to provide the secured environment here we are proposing three level authentications. During the registration phase three important authentic information are entered by the user. All the details are introduced in to the processing and then split into two shares. Each individual shares are stored in client and server side.

In the registration phase to do verification on user, reveal the two shares from client and server the user verify the server for phishing website and server verify the user authentication? The shares maintaining in two databases are encrypted one without knowing the encryption technique and share 2 one cannot get the card holder and card information.

The phishing websites cannot be detected in normal transaction procedure, but in our methodology while doing transaction one cannot enter their card information without uploading the correct information in the client side database also server should upload the registered information now the client shares and server shares are to be stacked together for getting the original authentic information. Now if the user communicating with phishing website they cannot produce the correct information.

This paper is organized as follows. Related work on smart card is reviewed in Section II. In section III describes Existing Methodology, in section IV deals with proposed methodologies, in section V describes Implementation and Section VI describes Conclusion and Future Work.

RELATED WORK

Rolf Oppliger, Ruedi Rytz, Thomas Holderegger et al [1] suggest Although current mechanisms protect against offline credential stealing attacks, effective protection against online channel-breaking attacks requires technologies to defeat man-in-the-middle (MITM) attacks, and practical protection against content-manipulation attacks requires transaction-authentication technologies.

Dr.V. Khanna, Professor & Dean, Department of IT, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: drvkannan62@yahoo.co.in

Dr.R. Udayakumar, Professor, Department of IT, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo et al [2] proposed an improvement to Chien et al.'s scheme to prevent from some weaknesses. However, the improved scheme is not only still susceptible to parallel session attack, but also insecure for changing the user's password in password change phase.

Accordingly, the current paper presents an enhancement to resolve such problems. As a result, the proposed scheme enables users to change their passwords freely and securely without the help of a remote server, while also providing secure mutual authentication1.

Sung Bum Pan, Daesung Moon, Younhee Gil, Dosung Ahn, and Yongwha Chung et al [3] propose an ultra-low memory fingerprint matching algorithm and implement it on a 32-bit smart card. We first evaluated both the number of instructions erected and memory requirement of each step of a typical fingerprint matching algorithm.

Then we developed a memory-efficient algorithm for the most memory consuming step alignment by doing more computations in the restriction of the real-time requirement. Our experimental results show that the proposed algorithm can reduce the required memory space by a factor of 62 and can be ere cured in real-time on a 32-bit smart card.

Chao Shen,, Zhongmin Cai, Xiaohong Guan, Youtian Du, and Roy A. Maxion, et al [4] presents a simple and efficient user authentication approach based on a fixed mouse-operation task. For each sample of the mouse-operation task, both traditional holistic features and newly-defined procedural features are extracted for accurate and fine-grained characterization of a user's unique mouse behavior. Distance-measurement and eigen space-transformation techniques are applied to obtain feature components for efficiently representing the original mouse feature space. Then a one-class learning algorithm is employed in the distance-based feature Eigen space for the authentication task. The approach is evaluated on a dataset of 5,550 mouse-operation samples from 37 subjects. Extensive experimental results are included to demonstrate the efficacy of the proposed approach, which achieves a false-acceptance rate of 8.74%, a false-rejection rate of 7.69% with a corresponding authentication time of 11.8 seconds. Two additional experiments are provided to compare the current approach with other approaches in the literature. Our dataset is publicly available to facilitate future research.

Wen-Shenq Juang et al [5] propose a novel user authentication and key agreement scheme using smart cards for multi-server environments with much less computational cost and more functionality. The major merits include: (1) users only need to register at the registration center once and can use permitted services in eligible servers; (2) the scheme does not need a verification table; (3) users can freely choose their passwords; (4) the computation and communication cost is very low; (5) servers and users can authenticate each other; (6) it generates a session key agreed by the user and the server; (7) it is a nonce-based scheme which does not have a serious time-synchronization problem.

Wen-Shenq Juang, Sian-Teng Chen, and Horng-Twu Liaw et al [6] propose a robust and efficient user authentication and key agreement scheme using smart cards. The main merits include the following: 1) the computation and communication cost is very low; 2) there is no need for any password or verification table in the server; 3) a user can freely choose and change his own password; 4) it is a nonce-based scheme that does not have a serious time-synchronization problem; 5) servers and users can authenticate each other; 6) the server can revoke a lost card and issue a new card for a user without changing his identity; 7) the privacy of users can be protected; 8) it generates a session key agreed upon by the user and the server; and 9) it can prevent the offline dictionary attack even if the secret information stored in a smart card is compromised.

Ren-Chiun Wang, Wen-Shenq Juang, and Chin-Laung Lei et al [7] proposed schemes, application servers do not need to maintain a verification table and this admired merit is not addressed by previous scholarship. Besides, the privacy of users is also addressed in Liao-Wang's scheme. In this article, we show that their schemes are not secure against the server spoofing and the impersonation attacks. Then we propose a robust user authentication scheme to withstand these attacks and keep the same merits.

Wen-Shenq Jaung et al [8] propose a novel three-party key exchange scheme using smart cards. The main merits of our scheme include: (1) there needs no verification, passwords or shared keys table in the trusted server; (2) users can freely choose and change their own passwords; (3) the communication and computation cost is very low; (4) two users can authenticate each other by the trusted server; (5) it generates a session key agreed between two users; (6) it is a nonce-based scheme which does not have a serious time synchronization problem.

EXISTING SYSTEM

Existing Authorization Procedure

When the buyer starts the transaction, they are sent to secure servers to complete the checkout process. The cardholder places an order at the merchant's site by clicking the "Send Order" button on the Review Order page during checkout.
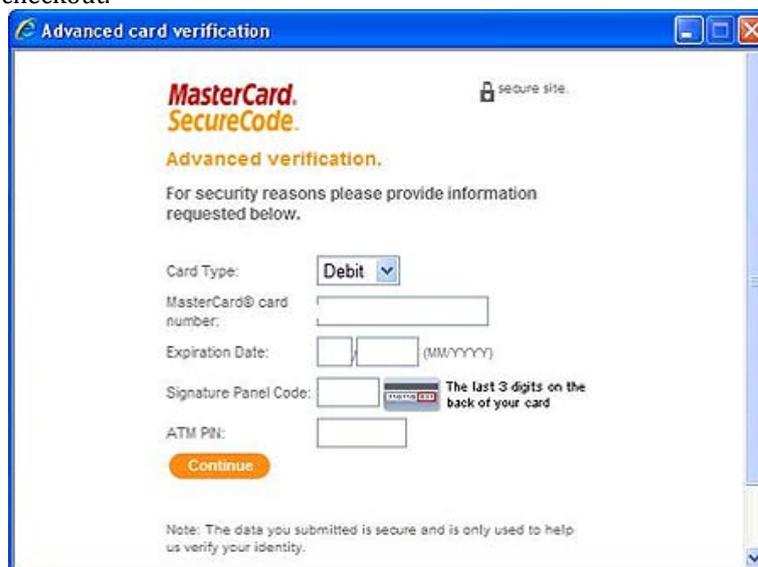

Fig. 1: Existing System

(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.

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.

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

PROPOSED METHODOLOGY

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

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.

Image Encryption and Sharing Procedure

Given Passport size photo is a shared secret image with M X N pixels. The dealer can derive shadows from M×N and generate 2 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.

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 MXN 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.

The Algorithm

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 $(x1,y1),(x2,y2).....(xn,ym)$ 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 share2.
Step5- Use step3 and split the odd pixels and even pixels in the manner that,.
(Odd, Odd), (Odd, Even) in share1 and (Even, Even)(Even, Odd) in share2.
Step6- Apply pixel positions in order for easy retrieval.
Step7- Apply pixel reversal to reverse the obtained pixels, in share1.
Step8- Store the reversed Pixel in matrix as image called share 1.
Step9- Apply pixel reversal to reverse the obtained pixels in share2.
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.

Zero Knowledge Authentications

Zero knowledge protocols are fascinating tool for the authentication verification. The two stack holders here are Prover and Verifier. The prover has to prove himself using queries generated by the verifier. If the prover failed to prove himself he is not authenticated. Zero knowledge protocol consist of two steps namely Identification and Operation. Identification schemes are methods by which a prover may prove his or her identity without revealing knowledge that may be used by an eavesdropper to impersonate the prover. The operation done by the verifier is to verify the details entered by the prover. When the card holder completed registration by entering the personal data is sent to host server.

The host server in turn verifies the pin number which is 1st phase of authentication. For second phase of authentication zero knowledge technique is used.

> p → v Prover to Verifier Code Passed
> v → p Verifier to Prover authentication set
> p → v Update zero knowledge code
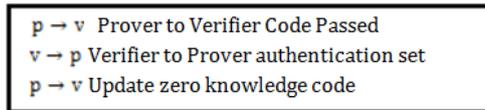
Proposed System

In our proposed system there are two phases Registration and Login Phase. During the registration phase the user should enter the three important authentic information and the information are encrypted and split into two parts.

Registration Phase

In the registration phase the system acquiring three different authentication information,

1. User Password(with key string)
2. Passport size image of card holder.
3. Zero knowledge code to be updated.

Here all these information are encrypted and split into two different parts. Each part is going to get stored in the client and server databases separately. The password is encrypted using substitution cipher algorithm. Then the obtained text is divided into two. The image of the user should get uploaded in the system. The image is shared using the algorithm and thus odd and even pixels are split into two shares. At last zero knowledge updated code is also split into two parts. One part of the all above three is get stored in client and another part will get stored in server database.
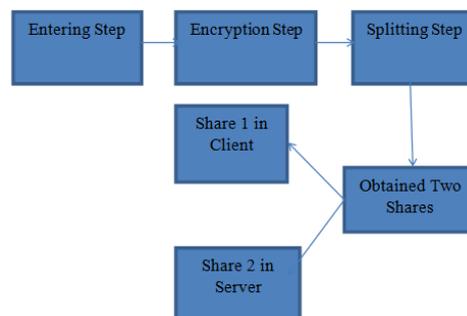

Fig. 2: Registration Phase

During the entering step input the required details such as password text, user image and the zero knowledge code. Then in the encryption step with the respective algorithms discussed above given inputs are encrypted. Then the encrypted outputs are splited into two halves. The two shares are get stored in client (user) and the server machine.

Login Phase

During login phase the user need to enter Share 1 details of the password, uploaded image and updated zero knowledge code, after that server reveal its share 2 both of the shares are going stacked together and finally apply the decryption algorithm on password, Image and Zero knowledge code then server verifies user password and client verifies the image and zero knowledge if both of them proved themselves now client can enter the card information for secured transaction. Decryption can be done on the password and image using the algorithms explained in the above section.
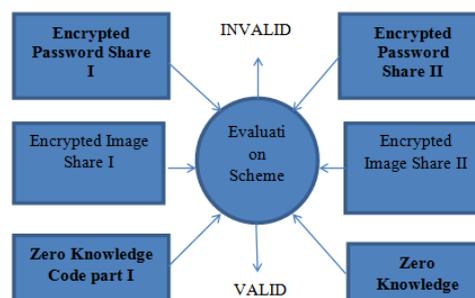

Fig. 3: Login and Verification Phase

IMPLEMENTATION

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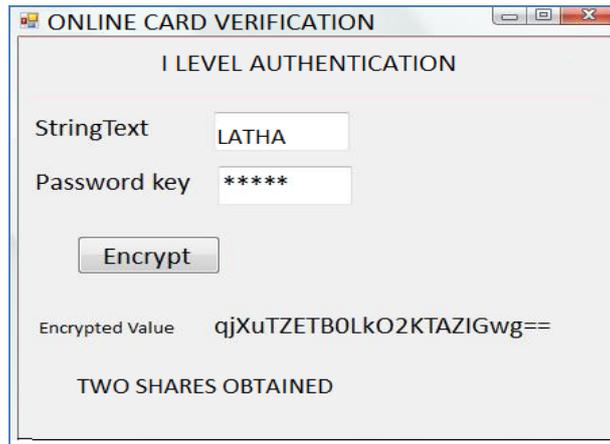

Fig. 4: I Level authentication

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

Fig. 5: Image Encryption

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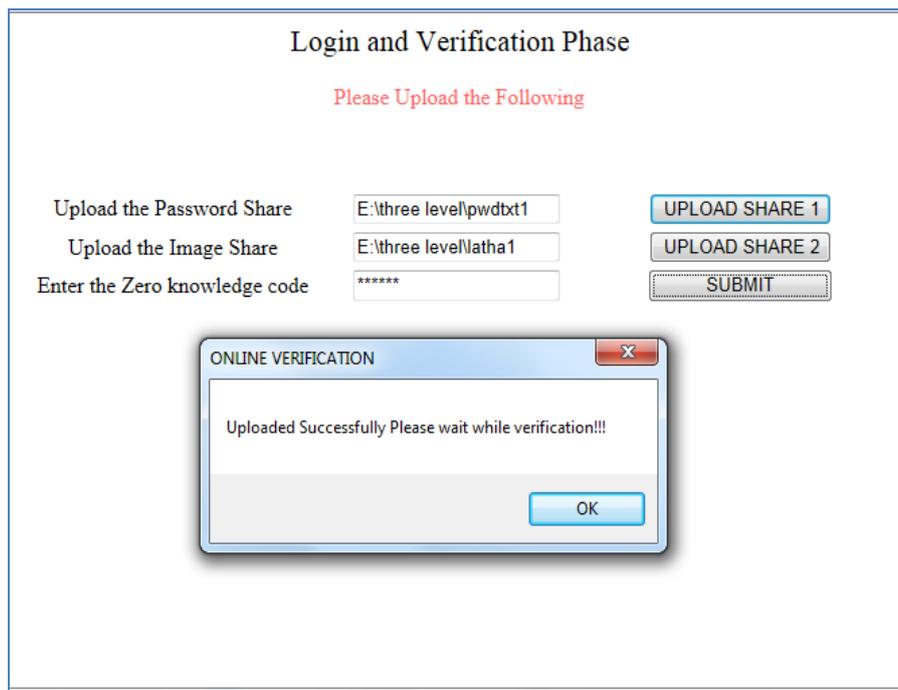

Fig. 6: Login and Verification phase

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.

CONCLUSION AND FUTURE WORK

The proposed methodology preserves smart card information of users using 3 levels of security. 1st level verifies whether the card holder is a valid person or not. If the person is not valid he cannot enter correct password and key for decryption. Second level of authentication is to verify whether the server is a genuine/secure website or a phishing website, If the website is a phishing then in that situation, the phishing website can't display the image for that specific user due to the fact that the image is generated by the stacking of two shares, one with the user and the other with the actual database of the website.

Third layer cross validates zero knowledge code which should get updated after the transaction is over. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. In future we can add biometric features with this methodology to enhance the security more. Also we can improve the cryptography by adding unique private key.

REFERENCES

[1] Tamilselvi, N., Krishnamoorthy, P., Dhamotharan, R., Arumugam, P., & Sagadevan, E. (2012). Analysis of total phenols, total tannins and screening of phytocomponents in Indigofera aspalathoides (Shivanar Vembu) Vahl EX DC. *Journal of Chemical and Pharmaceutical Research*, *4*(6), 3259-3262.

[2] Abraham, A.G., Manikandan, A., Manikandan, E., Jaganathan, S.K., Baykal, A., & Renganathan, P. (2017). Enhanced opto-magneto properties of Ni x Mg1–x Fe2O4 (0.0≤ x≤ 1.0) ferrites nano-catalysts. *Journal of Nanoelectronics and Optoelectronics*, *12*(12), 1326-1333.

[3] Barathiraja, C., Manikandan, A., Mohideen, A.U., Jayasree, S., & Antony, S.A. (2016). Magnetically recyclable spinel Mn x Ni 1– x Fe 2 O 4 (x=0.0–0.5) nano-photocatalysts: structural, morphological and opto-magnetic properties. *Journal of Superconductivity and Novel Magnetism*, *29*(2), 477-486.

[4] Kaviyarasu, K., Manikandan, E., Nuru, Z.Y., & Maaza, M. (2015). Investigation on the structural properties of CeO2 nanofibers via CTAB surfactant. *Materials Letters*, *160*, 61-63.

[5] Kaviyarasu, K., Manikandan, E., & Maaza, M. (2015). Synthesis of CdS flower-like hierarchical microspheres as electrode material for electrochemical performance. *Journal of Alloys and Compounds*, *648*, 559-563.

[6] Sachithanantham, P., Sa Nkaran, S., & Elavenil, S. (2015). Experimental study on the effect of rise on shallow funicular concrete shells over square ground plan. *International Journal of Applied Engineering Research*, *10*(20), 41340-41345.

[7] Jayalakshmi, T., Krishnamoorthy, P., Ramesh Kumar, G., &Sivaman, I.P. (2011). Optimization of culture conditions for keratinase production in Streptomyces sp. JRS19 for chick feather wastes degradation, *Journal of Chemical and Pharmaceutical Research*, *3*(4), 498-503.

[8] Kumarave, A., & Rangarajan, K. (2013). Routing alogrithm over semi-regular tessellations. In *2013 IEEE Conference on Information & Communication Technologies*, 1180-1184.

[9] Sonia, M.M.L., Anand, S., Vinosel, V.M., Janifer, M.A., Pauline, S., & Manikandan, A. (2018). Effect of lattice strain on structure, morphology and magneto-dielectric properties of spinel NiGdxFe2–xO4 ferrite nano-crystallites synthesized by sol-gel route. *Journal of Magnetism and Magnetic Materials*, *466*, 238-251.

[10] Rebecca, L.J., Susithra, G., Sharmila, S., & Das, M. P. (2013). Isolation and screening of chitinase producing Serratia marcescens from soil. *Journal of Chemical and Pharmaceutical Research*, *5*(2), 192-195.

[11] Banumathi, B., Vaseeharan, B., Rajasekar, P., Prabhu, N.M., Ramasamy, P., Murugan, K., & Benelli, G. (2017). Exploitation of chemical, herbal and nanoformulated acaricides to control the cattle tick, Rhipicephalus (Boophilus) microplus–a review. *Veterinary parasitology*, *244*, 102-110.

[12] Gopinath, S., Sundararaj, M., Elangovan, S., & Rathakrishnan, E. (2015). Mixing characteristics of elliptical and rectangular subsonic jets with swirling co-flow. *International Journal of Turbo & Jet-Engines*, *32*(1), 73-83.

[13] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2014). Efficiently measuring denial of service attacks using appropriate metrics. *Middle - East Journal of Scientific Research*, *20*(12): 2464-2470.

[14] Padmapriya, G., Manikandan, A., Krishnasamy, V., Jaganathan, S.K., & Antony, S.A. (2016). Enhanced Catalytic Activity and Magnetic Properties of Spinel MnxZn1–xFe2O4 (0.0 ≤ x ≤ 1.0)

Nano-Photocatalysts by Microwave Irradiation Route. *Journal of Superconductivity and Novel Magnetism, 29*(8): 2141-2149.

[15] Rajesh, E., Sankari, L.S., Malathi, L., & Krupaa, J.R. (2015). Naturally occurring products in cancer therapy. *Journal of pharmacy & bioallied sciences*, *7*(1), S181-S183.

[16] Vanangamudi, S., Prabhakar, S., Thamotharan, C., & Anbazhagan, R. (2014). Dual fuel hybrid bike. *Middle-East Journal of Scientific Research*, *20*(12): 1819-1822.

[17] Brindha, G., Krishnakumar, T., & Vijayalatha, S. (2015). Emerging trends in tele-medicine in rural healthcare. *International Journal of Pharmacy and Technology*, *7*(2): 8986-8991.

[18] Sharmila, S., Rebecca, L. J., Chandran, P. N., Kowsalya, E., Dutta, H., Ray, S., & Kripanand, N. R. (2015). Extraction of biofuel from seaweed and analyse its engine performance. *International Journal of Pharmacy and Technology*, *7*(2), 8870-8875.

[19] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2014). Using integrated circuits with low power multi bit flip-flops in different approch. *Middle-East Journal of Scientific Research*, *20*(12): 2586-2593.

[20] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2014). Virtual instrumentation based process of agriculture by automation. *Middle-East Journal of Scientific Research*, *20*(12): 2604-2612.

[21] Udayakumar, R., Kaliyamurthie, K.P., & Khanaa, T.K. (2014). Data mining a boon: Predictive system for university topper women in academia. *World Applied Sciences Journal*, *29*(14): 86-90.

[22] Anbuselvi, S., Rebecca, L.J., Kumar, M.S., & Senthilvelan, T. (2012). GC-MS study of phytochemicals in black gram using two different organic manures. *J Chem Pharm Res.*, *4*, 1246-1250.

[23] Subramanian, A.P., Jaganathan, S.K., Manikandan, A., Pandiaraj, K.N., Gomathi, N., & Supriyanto, E. (2016). Recent trends in nano-based drug delivery systems for efficient delivery of phytochemicals in chemotherapy. *RSC Advances*, *6*(54), 48294-48314.

[24] Thooyamani, K. P., Khanaa, V., & Udayakumar, R. (2014). Partial encryption and partial inference control based disclosure in effective cost cloud. *Middle-East Journal of Scientific Research*, *20*(12): 2456-2459.

[25] Lingeswaran, K., Prasad Karamcheti, S.S., Gopikrishnan, M., & Ramu, G. (2014). Preparation and characterization of chemical bath deposited cds thin film for solar cell. *Middle-East Journal of Scientific Research*, *20*(7), 812-814.

[26] Maruthamani, D., Vadivel, S., Kumaravel, M., Saravanakumar, B., Paul, B., Dhar, S.S., & Ramadoss, G. (2017). Fine cutting edge shaped Bi2O3rods/reduced graphene oxide (RGO) composite for supercapacitor and visible-light photocatalytic applications. *Journal of colloid and interface science*, *498*, 449-459.

[27] Gopalakrishnan, K., SundeepAanand, J., & Udayakumar, R. (2014). Electrical properties of doped azopolyester. *Middle-East Journal of Scientific Research*, *20*(11), 1402-1412.

[28] Subhashree, A.R., Parameaswari, P.J., Shanthi, B., Revathy, C., & Parijatham, B.O. (2012). The reference intervals for the haematological parameters in healthy adult population of chennai, southern India. *Journal of Clinical and Diagnostic Research: JCDR*, *6*(10), 1675-1680.

[29] Niranjan, U., Subramanyam, R.B.V., & Khanaa, V. (2010). Developing a web recommendation system based on closed sequential patterns. *International Conference on Advances in Information and Communication Technologies*, 171-179.

[30] Slimani, Y., Baykal, A., & Manikandan, A. (2018). Effect of Cr3+ substitution on AC susceptibility of Ba hexaferrite nanoparticles. *Journal of Magnetism and Magnetic Materials*, *458*, 204-212.

[31] Premkumar, S., Ramu, G., Gunasekaran, S., & Baskar, D. (2014). Solar industrial process heating associated with thermal energy storage for feed water heating. *Middle East Journal of Scientific Research*, *20*(11), 1686-1688.

[32] Kumar, S.S., Karrunakaran, C.M., Rao, M.R.K., & Balasubramanian, M.P. (2011). Inhibitory effects of Indigofera aspalathoides on 20-methylcholanthrene-induced chemical carcinogenesis in rats. *Journal of carcinogenesis*, *10*, 2011.

[33] Beula Devamalar, P.M., Thulasi Bai, V., & Srivatsa, S.K. (2009). Design and architecture of real time web-centric tele health diabetes diagnosis expert system. *International Journal of Medical Engineering and Informatics*, *1*(3), 307-317.

[34] Ravichandran, A.T., Srinivas, J., Karthick, R., Manikandan, A., & Baykal, A. (2018). Facile combustion synthesis, structural, morphological, optical and antibacterial studies of Bi1–xAlxFeO3 (0.0≤ x≤ 0.15) nanoparticles. *Ceramics International*, *44*(11), 13247-13252.

[35] Thovhogi, N., Park, E., Manikandan, E., Maaza, M., & Gurib-Fakim, A. (2016). Physical properties of CdO nanoparticles synthesized by green chemistry via Hibiscus Sabdariffa flower extract. *Journal of Alloys and Compounds*, *655*, 314-320.

[36] Kamalavathi, E., & Dr. Radhakrishnan, R. (2015). *International Scientific Journal on Science Engineering & Technology, 18*(8), 277-291.

[37] Beula Princy, S., & Dr. Duraisamy, S. (2016). Analysis of Retinal Images Using Detection of the Blood Vessels by Optic Disc and Optic Cup Segmentation Method. *International Scientific Journal on Science Engineering & Technology, 19*(2), 33-40.

[38] Kumaresan, D.C., & Dr. Selvan, P. (2016). A Survey on Two Port DC-DC Converter Topologies for Energy Preservation, *International Scientific Journal on Science Engineering & Technology, 19* (4), 66-73.

[39] Parikh, N. (2016). Partial Identification Framework for the Identification of Multi-Input Multi-Output System. *International Scientific Journal on Science Engineering & Technology, 19*(5), 79-86.

[40] Dr. Baskaran, S., Sampath, P., Sarathkumar, P., Sivashankar, S., & Vasanth Kumar, K. (2017). Implementation of Health Care Unitusing Web Server through IoT. *The SIJ Transactions on Computer Science Engineering & its Applications, 5*(2), 15-17.

[41] Rajkumar, G., Shalini, A., Sujatha, A., Vinothini, G., & Yuvarani, E. (2017). Tracking of Soldiers Location in any Environment using Intelligent Tracking and Health Indication System by using RSSI. *The SIJ Transactions on Computer Science Engineering & its Applications, 5*(3), 6-10.

[42] Mohammed, S., Dr. Ramkumar, L., & Rajasekar, V.R. (2017). A Novel Method using Convolutional Neural Network for Segmenting BrainTumor in MRI Images. *The SIJ Transactions on Computer Science Engineering & its Applications, 5*(3), 11-16.

[43] Sabarisha Malathi, P., & Dr.Vanathi, D. (2019). A Study of Data Storage Security Issues in Cloud Computing. *Bonfring International Journal of Software Engineering and Soft Computing, 9*(2), 5-7.

[44] Magesh Babu, M., Samundeeswari, R., Saranya, P., Sathiyapriya, R., & Susipriya, S. (2017).Analysis of Rapid Routing in FANET. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 5*(5), 1-5.

[45] Dhinakaran, M., Sivapriya, S., Thirugnanasoundari, K., & Vanmathi, V. (2017).Distributed System in Mobile Agent Communication. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 5*(5), 5-9.

[46] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2014). Wide area wireless networks-IETF. *Middle-East Journal of Scientific Research*, *20*(12), 2042-2046.

[47] Sundar Raj, M., Saravanan, T., & Srinivasan, V. (1785). Design of silicon-carbide based cascaded multilevel inverter. *Middle-East Journal of Scientific Research*, *20*(12), 1785-1791.

[48] Achudhan, M., & Prem Jayakumar, M. (2014). Mathematical modeling and control of an electrically-heated catalyst. *International Journal of Applied Engineering Research*, *9*(23).

[49] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2013). Application of pattern recognition for farsi license plate recognition. *Middle-East Journal of Scientific Research*, *18*(12), 1768-1774, 2013.

[50] Jebaraj, S., & Iniyan S. (2006). Renewable energy programmes in India. *International Journal of Global Energy,* 26: 232-257.