Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2018 13 (3): 1101-1107

Biometric Authentication for Cloud Service Provider in Multiple Cloud Storage System

M. Ramamoorthy, N. Ayyanathan, M. Padma Usha

Received: 22 Jan 2018 ▪ Revised: 27 March 2018 ▪ Accepted: 20 April 2018

Abstract: Cloud storage services provides users to store large amount of files. Distributed clients can also access the file storage. To provide integrity, controllable outsourcing and auditing on outsourced file, we used a scheme called identity-based data outsourcing (IBDO) which provide more advantageous when compared to existing systems. In IBDO scheme, the users allows the designated entities to upload data on behalf of the user. The entities are authorized and identified using their identities. The IBDO also promotes comprehensive auditing which allows the user to check the information based on type and consistence of outsourced files and also the MAC address and IP address are checked. To provide more security we added biometric authentication called fingerprint analysis and to overcome security threats, we proposes multiple cloud storage system using split and merge technique, e.g., a file is divided into multiple fragments and stored in multiple clouds.

Keywords: Cloud Storage, Data Integrity, Data Outsourcing, Identity-based Cryptography, Security.

INTRODUCTION

Cloud storage is a model of data storage in which the digital data is stored in logical pools. The internet provides the connection between the user's computer and the database. Cloud holds data from many different users and organizations. The service allows the users to store files online, so that they can access them from any location via the internet. The cloud storage providers are responsible for keeping the data available and accessible. Clients send files to a data server maintained by a cloud provider instead of storing it on their own hard drives. People and organizations buy or lease storage capacity from the providers to store user, organization or application data. Cloud storage is highly fault tolerant through redundancy and distribution of data. It is made up of many distributed resources. When the file was uploaded, it is stored at more locations which will increase the risk of unauthorized physical access to the data. In the existing system, they used the POS like schemes which is not supporting for the data log related auditing in data possession proof, for that we proposes Identity Based Data Outsourcing(IBDO) scheme which provides comprehensive auditing i.e., not only permits integrity auditing but also allows to audit the data on type and consistence of outsourcing files. The traditional approach is used to store the files in the cloud.

In that, by knowing the user's ID and the password the unauthorized proxies may access a file which is uploaded by owners. To provide more security, we proposes one of the biometric authentication called fingerprint analysis for the user's authentication and to overcome the data integrity, we proposes multiple cloud storage system invoking split and merge concept, that is the file which is to be stored is divided into multiple fragments and stored in multiple clouds and also before uploading the file, the data is encrypted and then stored on the cloud.

M. Ramamoorthy, Assistant Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: saimoorthy123@gmail.com

N. Ayyanathan, Associate Professor, Master of Computer Applications, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. E-mail: n.ayyanathan@crescent.education

M. Padma Usha, Assistant Professor, Electronics and Communication Engineering, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, India. E-mail: padmausha@crescent.education

OUR CONTRIBUTION

To manage the problems in securing outsourced data, Identity Based Data Outsourcing (IBDO) scheme is used in this paper. For the effective storage of outsourced file, this paper proposes multiple cloud storage system invoking split and merge technique and to make the machine identify the data owner and the designated entities, effective fingerprint analysis is promoted.

IDENTITY MANAGEMENT – DATA OWNERS / DEDICATED PROXIES

Fingerprint Feature Extraction

Fingerprint based biometric authentication is an important and widely used biometric type authentication because of its cost, accuracy and feasibility. In our proposed system, the user fingerprint feature are extracted and verified using Minutiae Map algorithm (MM) [1]. Minutiae Map algorithm identifies the fingerprint ridges and extracts the bifurcation and termination values from the input fingerprint image.

Ridge termination is the point at which ridge ends. Bifurcation is the point at which ridge splits into two halves which is shown in the below figure. Our proposed system provides the respective user fingerprint total bifurcation,

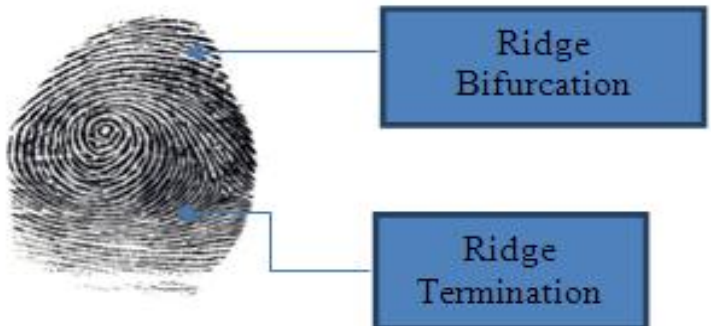

Fig.1: Ridge Bifurcation and Ridge Termination

Termination values along with its location (X, Y coordinates) and stores in the database during user registration.

In our proposed system, ideal thinned ridge is considered. We assume usually a thinned ridge will have a value 1 or 0.

The algorithm uses 3*3 windows to scan the image and the bifurcation and termination in the final output image shall be represented by a dot. Let's consider (x,y) denote the pixel on the thinned ridge and N_0, n_1, ……N_7 denote its neighbours.

A pixel (x,y) is a ridge ending if,

$$\sum_{i=0}^{7} Ni = 1$$

A pixel (x,y) is a ridge bifurcation if,

$$\sum_{i=0}^{7} Ni > 2$$

DATA OWNER / DEDICATED PROXIES BEHAVIOUR ANALYSIS

In this module the data owner / dedicated proxies behaviour is been analyzed. For this we keep a log of origin, file types, consistence of outsourced. We use techniques to detect the MAC address whenever the data owner / dedicated proxies access. If they access from different machines or upload / access different file types an alert e-mail would be sent to the data owner. On approval by the data owner the dedicated proxies would be allowed to access inside the application.

ELIMINATES COMPLEX CRYPTOGRAPHIC CERTIFICATES

To eliminate complex cryptographic certificates we used SHA algorithm for converting the plain text to cipher text.

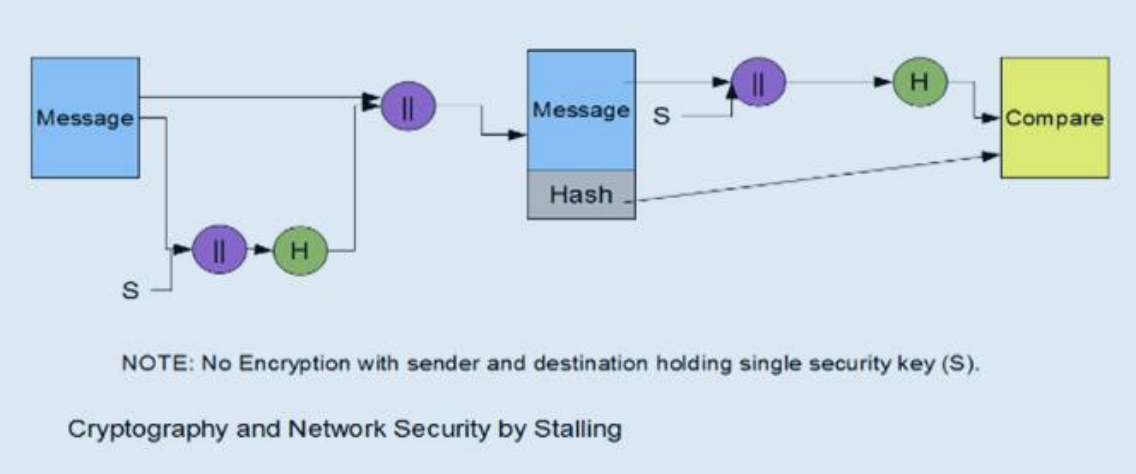

Fig. 2: Cryptography and Network with sender and destination

- Step 1: Append Padding Bits….

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512.

- Step 2: Append Length....

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

- Step 3: Prepare Processing Functions….

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

- Step 4: Prepare Processing Constants....

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)

- Step 5: Initialize Buffers….

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0

- Step 6: Processing Message in 512-bit blocks (L blocks in total message)….

This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.

Input and predefined functions:

M[1, 2, ..., L]: Blocks of the padded and appended message f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions K(0), K(1), ..., K(79): 80 Processing Constant Words

H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values

- Step 6: Pseudo Code….

For loop on k = 1 to L
(W (0), W (1)... W (15)) = M[k] */* Divide M[k] into 16 words */*
For t = 16 to 79 do:
W (t) = (W (t-3) XOR W (t-8) XOR W (t-14) XOR W (t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4
For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,
C = B<<<30, B = A, A = TEMP
End of for loop

H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop

SPLIT AND MERGE TECHNIQUE

Cloud Storage usually contains business-critical data and processes, hence high security is the only solution to retain strong trust relationship between the cloud users and cloud service providers. Thus to overcome the security threats, this paper proposes multiple cloud storage. Thus the common forms of data storage such as files and databases of a specific user is split and stored in the various cloud storages (e.g. Cloud A and Cloud B).

Databases consists of tables, rows and columns. Databases are easy to store in multiple cloud storages. Our application will act as a combiner and store different parts of the table such as rows and columns in multiple clouds using Vertical fragmentation and horizontal fragmentation. These rows and columns will be converted into hash value using hash function algorithm and stored in each clouds. During response our application combines the data and sends to the verifier.

Files are stored in multiple clouds using cryptographic data splitting. The file is split into fragments and stored in distinct cloud servers with encrypted key. Thus once the authorized token for the specific file is requested, searchable encryption allows keyword search on encrypted data and combines the fragments. This is sent to the verifier.

DATA STORAGE

A cloud server is defined as an entity which contains huge data storage managed by cloud service provider. This paper focuses on providing high security for user data in public cloud storages because there is a huge demand of security prospects in public cloud storages. Security threats may include some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud and cloud based attacks.

For Cloud storage we have configured public clouds. Public clouds is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration. The service provides 2 gigabytes (GB) of storage for free and up to 100 GB on various for-fee plans. Public clouds is cloud storage service that enables users to store files on remote cloud servers and the ability to share files within a synchronized format.

RELATED WORK

Identity based data outsourcing scheme is introduced by YujueWang [1] to manage problems in securing outsourced data. This scheme only permits authorized dedicated proxies to upload data to the cloud storage on the behalf of the user. Users and dedicated proxies can able to upload data only by using some of their identities. This scheme provides strong security in data integrity. GiuseppeAteniese [4] proposed secured Provable data possession technique. It is based on symmetric key cryptography, while not requires any bulk encryption. It supports modification, deletion and append. Through this technique client can check the data stored on server is secure or not. The first efficient Identity-Based Encryption (IBE) scheme is introduced by Brent Waters [34] and reduced the risk of Bilinear Diffie-Hellman (BDH) problem. It is fully secure without random oracles. C.Wang [10] proposed a system for secure cloud storage supporting privacy-preserving public auditing. Users use cloud storage for storing their data rather than local storage. Public auditability for cloud storage is enabled for third party auditor to check the integrity of outsourced data. Yong Yu, Man Ho Au∗, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and GeyongMin[28] described about “Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage”. Remote data integrity checking proves to the users that their data stored in a cloud storage is secured. A new construction of identity-based (ID-based) RDIC protocolis proposed in this system and it make use of key-homomorphic cryptographic primitive.

It reduces the complexity of system and cost. In the proposed system, information which is stored in the data storage i.e. cloud storage cannot be leaked during the process of Remote data integrity checking (RDIC).G. Ateniese describes about “Provable Data Possession at Untrusted Stores” [4]. The data of the user is stored at an untrusted server sometimes data cannot be retrieved. To tackle this problem, a model for provable data possession is proposed. K. Yang and X. Jia [3] describes, “Data storage auditing service in cloud computing: challenges, methods and opportunities”. To know that data in cloud storage stored correctly, an independent auditing service is needed. This type of problem is investigated in the proposed system.B. Wang, B. Li, and H. Li [10] proposed, “Panda: Public auditing for shared data with efficient user revocation in the cloud”. Using cloud storage users can store data and also can make modifications in it. Users can share data as a group. Once the user signed up a block, want to again re-sign by the existing

user. The proposed system uses the idea of proxy re-signatures, in this cloud is allowed to re-sign the blocks without the existing users. So, the user doesn't need any re-sign blocks by themselves. The data is always audited by a public verifier without retrieving entire data in the cloud.

CONCLUSION

In this paper, we proposed multiple cloud storage system invoking split and merge technique. Only authorized designated entities can upload files on the behalf of the user. Fingerprint analysis is used for user's identification. Files are encrypted and uploaded in the cloud storage. Uploaded files are divided and stored in multiple clouds. The uploaded files can be viewed by the users after merging the files using the key, generated during the encryption. Like this, files are uploaded, stored and retrieved in a secured way. So, unauthorized proxies cannot access the files and the integrity of the file was improved in a better way.

REFERENCES

[1] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique. *Indian Journal of Science and Technology*, *6*(6), 4767-4771.

[2] Udayakumar, R., Kumaravel, A., & Rangarajan, K. (2013). Introducing an efficient programming paradigm for object-oriented distributed systems. *Indian Journal of Science and Technology*, *6*(5S), 4596-4603.

[3] Mageswaran, S.U., & Sekhar, N.G. (2013). Reactive power contribution of multiple STATCOM using particle swarm optimization. *International Journal of Engineering & Technology*, *5*(1), 122-126.

[4] Ristono, A., & Budi, P. (2019). Design of Reliable and Efficient Manchester Carry Chain Adder based 8-BIT ALU for High Speed Applications. *Journal of VLSI Circuits And Systems, 1*(1), 1-4.

[5] Anoop, T.R., & Mini, M.G. (2015). Altered Fingerprint Matching Using Ridge Texture and Frequency in the Unaltered Region. *Bonfring International Journal of Advances in Image Processing, 5*(2), 06-09.

[6] Sindhuja, R. (2019). An Analysis of Image Segmentation techniques. *Journal of Computational Information Systems, 15*(1), 171-175.

[7] Sudarsanam, P. (2019). Location Oriented Android Discount Tracker. *Journal of Computational Information Systems, 15*(2), 15-21.

[8] Sharma, D.K. (2019). Performance Evaluation of SFIG and DFIG Based Wind Turbines. *Journal of Computational Information Systems, 15*(2), 45-53.

[9] Nemmani, D.S. (2019). SCADA System Application for Power Distribution in Hyderabad City. *Journal of Computational Information Systems, 15*(3), 79-88.

[10] Gireesha. B, (2018). A Comparative Performance Evaluation of Swarm Intelligence Techniques *Journal of Computational Information Systems, 14*(4), 14 - 20.

[11] Santhanaraj, M., Prasanth, S., Sarath Kumar, K., Vishnu Chander, R., & Vijayaragavan, T. (2015). Segmentation and Detection of Magnetic Resonance Image Based on K-Mean Algorithm. *International Journal of Advances in Engineering and Emerging Technology, 7*(3), 133-138.

[12] Eswari, K.E., and Arunkumar, R.K. (2014). Wi-Fi Technology. *Excel International Journal of Technology, Engineering and Management, 1*(2), 42-45.

[13] Job, D., & Paul, V. (2016). Recursive Backtracking for Solving 9*9 Sudoku Puzzle. *Bonfring International Journal of Data Mining, 6*(1), 07-09.

[14] Giri, R.K., & Saikia, M. (2013). Multipath routing for admission control and load balancing in wireless mesh networks. *International Review on Computers and Software*, *8*(3), 779-785.

[15] Padmapriya, G., Manikandan, A., Krishnasamy, V., Jaganathan, S.K., & Antony, S.A. (2016). Spinel NixZn1− xFe2O4 (0.0≤ x≤ 1.0) nano-photocatalysts: synthesis, characterization and photocatalytic degradation of methylene blue dye. *Journal of Molecular Structure*, *1119*, 39-47.

[16] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., & Sundar Raj, M. (2013). Analysis of chaotic DC-DC converter using wavelet transform. *Middle-East Journal of Scientific Research*, *16*(12), 1813-1819.

[17] Lokesh, K., Kavitha, G., Manikandan, E., Mani, G.K., Kaviyarasu, K., Rayappan, J.B.B., ... & Maaza, M. (2016). Effective ammonia detection using n-ZnO/p-NiO heterostructured nanofibers. *IEEE Sensors Journal*, *16*(8), 2477-2483.

[18] Abraham, A.G., Manikandan, A., Manikandan, E., Vadivel, S., Jaganathan, S.K., Baykal, A., & Renganathan, P.S. (2018). Enhanced magneto-optical and photo-catalytic properties of transition metal cobalt (Co2+ ions) doped spinel MgFe2O4 ferrite nanocomposites. *Journal of Magnetism and Magnetic Materials*, *452*, 380-388.

[19] Kennedy, J., Fang, F., Futter, J., Leveneur, J., Murmu, P.P., Panin, G.N., & Manikandan, E. (2017). Synthesis and enhanced field emission of zinc oxide incorporated carbon nanotubes. *Diamond and Related Materials*, *71*, 79-84.

[20] Teresita, V.M., Manikandan, A., Josephine, B.A., Sujatha, S., & Antony, S.A. (2016). Electromagnetic properties and humidity-sensing studies of magnetically recoverable LaMg x Fe 1− x O 3− δ perovskites nano-photocatalysts by sol-gel route. *Journal of Superconductivity and Novel Magnetism*, *29*(6), 1691-1701.

[21] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of pure and doped bis thiourea zinc acetate: Semiorganic nonlinear optical single crystals. *Current applied physics*, *9*(5), 1054-1061.

[22] Jayalakshmi, V., & Gunasekar, N.O. (2013). Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag/swell. *International Conference on Energy Efficient Technologies for Sustainability*, 1036-1040.

[23] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). Optical ring architecture performance evaluation using ordinary receiver. *Indian Journal of Science and Technology*, *6*(6), 4742-4747.

[24] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). Performance analysis of resilient ftth architecture with protection mechanism. *Indian Journal of Science and Technology*, *6*(6), 4737-4741.

[25] Saravanan, T., Srinivasan, V., & Sandiya, V.P. (2013). A two stage DC-DC converter with isolation for renewable energy applications. *Indian Journal of Science and Technology*, *6*(6), 4824-4830.

[26] Sundarraj, M. (2013). Study of compact ventilator. *Middle-East Journal of Scientific Research*, *16*(12), 1741-1743.

[27] Thema, F.T., Manikandan, E., Gurib-Fakim, A., & Maaza, M. (2016). Single phase Bunsenite NiO nanoparticles green synthesis by Agathosma betulina natural extract. *Journal of alloys and compounds*, *657*, 655-661.

[28] Sathyaseelan, B., Manikandan, E., Sivakumar, K., Kennedy, J., & Maaza, M. (2015). Enhanced visible photoluminescent and structural properties of ZnO/KIT-6 nanoporous materials for white light emitting diode (w-LED) application. *Journal of Alloys and Compounds*, *651*, 479-482.

[29] Gopalakrishnan, K., Prem Jeya Kumar, M., Sundeep Aanand, J., & Udayakumar, R. (2013). Analysis of static and dynamic load on hydrostatic bearing with variable viscosity and pressure. *Indian Journal of Science and Technology,* 6(6), 4783-4788.

[30] Prabhu, M.R., Reji, V., & Sivabalan, A. (2012). Improved radiation and bandwidth of triangular and star patch antenna. *Research Journal of Applied Sciences, Engineering and Technology*, *4*(12), 1740-1747.

[31] Arumugam, S. and Ramareddy, S. (2012). Simulation comparison of class D/ Class E inverter fed induction heating. *Journal of Electrical Engineering*, 12(2), 71-76.

[32] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). High data rate for coherent optical wired communication using DSP. *Indian Journal of Science and Technology*, *6*(6), 4772-4776.

[33] Nagarajan, C., & Madheswaran, M. (2012). Experimental Study and Steady State Stability Analysis of CLL-T Series Parallel Resonant Converter with Fuzzy Controller using State Space Analysis. *Iranian Journal of Electrical and Electronic Engineering*, *8*(3): 259-267.

[34] Gopalakrishnan, K., PremJeya Kumar, M., SundeepAanand, J., & Udayakumar, R. (2013). Thermal properties of doped azopolyester and its application. *Indian Journal of Science and Technology*, *6*(6), 4722-4725.

[35] Kumaravel A., Meetei O.N. (2013). An application of non-uniform cellular automata for efficient cryptography. *Indian Journal of Science and Technology*, *6*(5): 4560-4566.

[36] Kumaravel, A., & Pradeepa, R. (2013). Layered approach for predicting protein subcellular localization in yeast microarray data. *Indian Journal of Science and Technology*, *6*(5S), 4567-4571.

[37] Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2016). Synthesis and analytical applications of photoluminescent carbon nanosheet by exfoliation of graphite oxide without purification. *Journal of Materials Science: Materials in Electronics*, *27*(12), 13080-13085.

[38] Mathubala, G., Manikandan, A., Antony, S.A., & Ramar, P. (2016). Photocatalytic degradation of methylene blue dye and magneto-optical studies of magnetically recyclable spinel NixMn1-xFe2O4 (x= 0.0–1.0) nanoparticles. *Journal of Molecular Structure*, *1113*, 79-87.

[39] Manikandan, E., Kennedy, J., Kavitha, G., Kaviyarasu, K., Maaza, M., Panigrahi, B.K., & Mudali, U.K. (2015). Hybrid nanostructured thin-films by PLD for enhanced field emission performance for radiation micro-nano dosimetry applications. *Journal of Alloys and Compounds*, *647*, 141-145.

[40] Kumaravel, A., & Meetei, O.N. (2013). An application of non-uniform cellular automata for efficient cryptography. *IEEE Conference on Information & Communication Technologies*: 1200-1205.

[41] Langeswaran, K., Gowthamkumar, S., Vijayaprakash, S., Revathy, R., & Balasubramanian, M.P. (2013). Influence of limonin on Wnt signalling molecule in HepG2 cell lines. *Journal of natural science, biology, and medicine*, *4*(1), 126-133.

[42] Srinivasan, V., & Saravanan, T. (2013). Analysis of harmonic at educational division using CA 8332. *Middle-East Journal of Scientific Research*, *16*(12), 1768-73.

[43] Josephine, B.A., Manikandan, A., Teresita, V.M., & Antony, S A. (2016). Fundamental study of LaMg x Cr 1− x O 3− δ perovskites nano-photocatalysts: sol-gel synthesis, characterization and humidity sensing. *Korean Journal of Chemical Engineering*, *33*(5), 1590-1598.

[44] Saravanan, T., Saritha, G., & Udayakumar, R. (2013). Robust H-Infinity Two Degree of Freedom Control for Electro Magnetic Suspension System. *Middle-East Journal of Scientific Research*, *18*(12), 1827-1831.

[45] Rajasulochana, P., Dhamotharan, R., Murugakoothan, P., Murugesan, S., & Krishnamoorthy, P. (2010). Biosynthesis and characterization of gold nanoparticles using the alga Kappaphycus alvarezii. *International Journal of Nanoscience*, *9*(05), 511-516.

[46] Slimani, Y., Güngüneş, H., Nawaz, M., Manikandan, A., El Sayed, H. S., Almessiere, M. A., & Baykal, A. (2018). Magneto-optical and microstructural properties of spinel cubic copper ferrites with Li-Al co-substitution. *Ceramics International*, *44*(12), 14242-14250.

[47] Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., & Maaza, M. (2016). Rice husks as a sustainable source of high quality nanostructured silica for high performance Li-ion battery requital by sol-gel method–a review. *Adv. Mater. Lett*, *7*(9), 684-696.

[48] Ilayaraja, K., & Ambica, A. (2015). Spatial distribution of groundwater quality between injambakkamthiruvanmyiur areas, south east coast of India. *Nature Environment and Pollution Technology*, *14*(4), 771-776, 2015.

[49] Sharmila, S., Rebecca, L. J., Das, M.P., & Saduzzaman, M. (2012). Isolation and partial purification of protease from plant leaves. *Journal of Chemical and Pharmaceutical Research*, *4*(8), 3808-3812.

[50] Rajakumari, S.B., & Nalini, C. (2014). An efficient cost model for data storage with horizontal layout in the cloud. *Indian Journal of Science and Technology*, *7*(3), 45-46.