Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2018 13 (3): 698-704

Secure Message Authentication Using HMAC

K. Sivaraman, G. Kavitha

Received: 02 Jan 2018 ▪ Revised: 07 March 2018 ▪ Accepted: 30 March 2018

Abstract: RFID and Wireless Sensor Networks exemplify computationally constrained environments, where the compact nature of the components cannot support complex computations or high communication overhead. On the other hand, such components should support security applications such as message integrity, authentication, and time stamping. The latter are efficiently implemented by Hash Message Authentication Codes (HMAC). As clearly stated in the literature, current approved implementations of HMAC require resources that cannot be supported in constrained components. An approach to implement a compact HMAC by the use of stream ciphering is presented in this paper.

Keywords: HMAC, Radio Frequency Identification (RFID), Stream Ciphering, Sequential Processing.

INTRODUCTION

MAC and Challenge-Response Interrogation

MESSAGE integrity and authenticity, and replay prevention, are essential in security-related communications. Here, a receiver is expected to be able to verify that a received message, originally transmitted by a valid source, was not changed. Also, the receiver has to verify that the message was not transmitted by a cloned source, and is not a retransmission of an originally genuine message transmitted in the past by a valid source. Technically, verifying message integrity and authenticity is based on the receiver's ability to prove to itself that the transmitter stores a valid secret key that was used when the message was transmitted. Surely, symmetric and asymmetric cryptographic schemes can also be used in satisfying the above. In this paper, we treat the case where the facility at the data source has limited resources. In such environments, message integrity and authenticity is usually verified using Message Authentication Code (MAC). *MAC(M,K)* is a one-way transformation of the message M and a secret key K shared with the verifier. The values M and *MAC(M,K)* are both sent to the verifier. Upon receiving these values, the verifier generates himself a value *MAC(M,K)* based on the received M and the value of K known to him. If *MAC(M,K)* = *MAC(M,K)*, the verifier decides that the message is authentic and equals its original value. If an attacker has access to an oracle which possesses K and generates MACs for messages M chosen by the attacker, it should be infeasible to guess the MAC value for any new message not interrogated before. To prevent illegal replaying, there is also a need for a time-dependent proof. This is achieved by a challenge-response interrogation procedure, as depicted in Fig. 1.

Subsequently, the interrogated component transmits:

1) The component's public key PK, which is an encrypted version of K issued by the system manager and stored in the component, 2) *M,* and 3) *CR*.

Upon receiving the above three values, the interrogator performs the operations shown at the bottom of the figure. The interrogator first retrieves K out of the received PK, using a system decryption key. In practice, the system decryption key is not necessarily stored at the interrogator's facility. Here, the interrogation operations can be performed in an external secure place. Under another version, the key *K* of the interrogated component is retrieved from a secured network, rather than being recovered by decrypting a value *PK* submitted by the component. The same mechanism can also be used in access control, preventing illegal writings of a message M into the component, by still executing a MAC operation in the component. The comparison of the MAC values is done in the component. Upon success, *M* is allowed to be written

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

G. Kavitha, Assistant Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

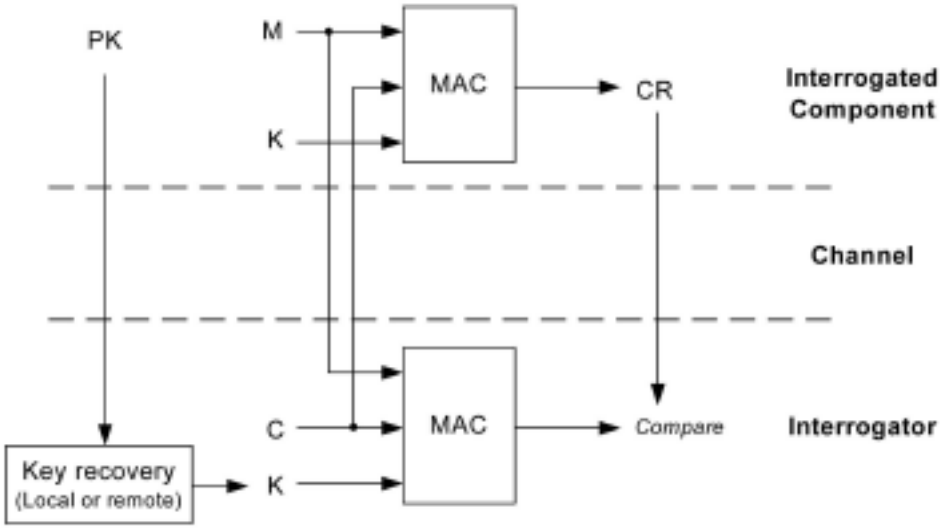

Fig. 1: MAC-based challenge-response procedure

There are other variations to the circuit of Fig. 1. For example, in some cases, there is no message M to be authenticated, and the purpose of the interrogation is just to verify that the interrogated component really has the valid *K* associated with *PK*. In other cases, like prevention of car-theft, K is installed in advance in the interrogated component and the interrogating transmitter-receiver. Here, PK and its handling are redundant.

MAC and HMAC in the Context of This Paper

As described above, *MAC(M,K)* is a one-way transformation of the message M and a secret key K. The implementation this transformation can be based on various approaches. Hash Message Authentication Code (HMAC) is a hash transformation parameterized with a secret key. That is, it is an implementation of *MAC(M,K)*. In this paper, we treat a standardized HMAC. The security of such implementations has been revised stating that the attacks "do not contradict the security proof of HMAC, but they improve our understanding of the security of HMAC based on the existing cryptographic hash functions." The suggested implementation of HMAC is of the form

$$HMAC(text, K) = H[K_{out} \| H(K_{in} \| text)],$$

Where,

- H is a cryptographic hash function.
- *Kin* and *Kout* are two keys, derived from K.
- ‖ denotes a concatenation.
- *text* is the text to be hashed together with K. In relation to the challenge response procedure of Fig. 1, we adopt an implementation where text= *C‖M*.

The following is one recommended way of constructing *Kin* and *Kout* out of *K*. Let *K* be b-bytes long. opad and ipad denote b-byte values, consisting, respectively, of b repetitions of the byte 01011100 and 00110110. Then, Kout = K Θopad and Kin =K Θipad, where Θ denotes an XOR.

Any standard hash (e.g., SHA-1), as well as the above specified HMAC implementation, is specified in a way which facilitates the processing of a relatively long text, by iteratively processing it in parts. That is, text is broken into sections, which are processed one at a time. Each such section is processed by a one-way block transformation whose parameters are limited in size to that of the processed section. This general approach is especially suitable when dealing with constrained hardware resources. Even if text is a few hundred of bits long, where K is about 100 bits, it would still be recommended to process text in parts. This is the approach taken in this paper.

Interrogation in Highly Constrained Environments

Radio Frequency IDentification (RFID) facilitates, by definition, identification by wireless communications. In many applications an RFID tag is required to prove the authenticity of data it transmits.

The use of RFID in medical applications presents special security demands.

Two main constraints are considered here: 1) Costs: Wide adoption of RFID is crucially dependent on the price of a tag.

This is translated into a limited number of logic gates used in the tag. 2) Power consumption: An RFID tag is operated by a magnetic field radiated from the reader. It does not have its own power source. This puts a severe limitation on the number of gates that can operate simultaneously.

Related Work and the Structure of the Paper

Compact MAC implementations in constrained environments are of the essence. Possible implementations of hash in constrained environments, based on block ciphers, are surveyed. Here, a one-way block transformation, based on a stream cipher, is first implemented as a stand-alone universal circuit.

This can then also be turned into an HMAC implementation. This turns into HMAC transformation by implementing HMAC(text;K)=H[Kout‖H(Kin‖text)].

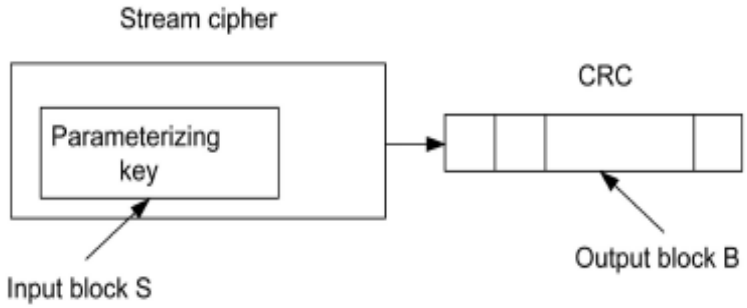

Fig. 2: One-way block transformation based on stream cipher

ONE-WAY TRANSFORMATIONS BASED ON STREAM CIPHERING

Block Transformation based on Stream Cipher

A stream cipher exhibits the following features:

1. It produces a pseudorandom keystream output which is very strongly dependent on a parameterizing secret key S. (We purposely denote the parameterizing key differently from the secret key K used in the intended MAC application.) A minor change in S causes major output changes.
2. The underlying security of the cipher is measured in terms of the difficulty in retrieving S, given an output keystream of any feasible length. The circuit of **Fig. 2** presents an approach for utilizing the above two features of a stream cipher in implementing a one-way block transformation. The input block S, acting as the parameterizing key of the stream cipher, yields a keystream that enters a Cyclic Redundancy Code (CRC) circuit. The circuit is clocked for a number of cycles that is significantly larger than the length of S. The final content of the CRC register is the output block B. That is, the circuit transforms the input block S into the output block B.

Security Considerations

1) The One-Way Strength of the Transformation

Surely, recovering S from a compressed version of the cipher's output keystream, even if the compression is based on a simple linear CRC, cannot have a lower complexity than the recovery of S from a fully given keystream. As the latter is expected to be infeasible for secure cipher, the irreversibility of the transformation of **Fig. 2** is at least as strong as the underlying security of the cipher.

2) Related-Key Attacks

A related-key attack is based on the assumption that an attacker observes the operation of a cipher under different keys, where some relationship among the keys is known to him. It is essential that the same key never be used more than once in a stream cipher. The best would be to use a randomly generated key for each new use of the cipher.

Related-key attacks on stream ciphers concern key scheduling. This relates to applications where practical circumstances dictate the use a fixed key master key, which is randomized in a key-scheduling process, to yield a different key for each communication session.

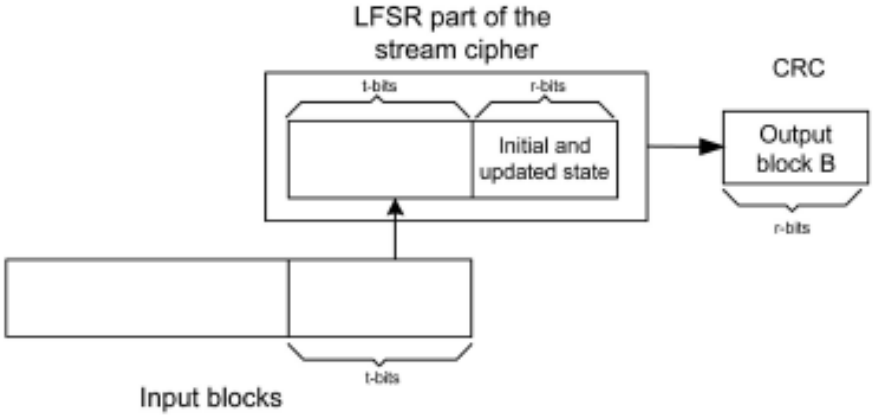

Fig. 3: Processing the input in parts and where H is based on stream ciphering

ITERATIONS OF THE ONE-WAY BLOCK TRANSFORMATION

Implementing an HMAC

General hashing means transforming chained input blocks into an output block of a fixed, relatively small, length. This is performed by iterations, where input blocks enter one at a time and are combined with an accumulated value that consists of the hashing performed so far. When the iterations are complete (i.e., the entire input chain has been processed) the output should be the hash of the entire input.

An approach for iterating a one-way block transformation, based on stream ciphering, is depicted in **Fig. 3.** Here, the Linear Feedback Shift Register (LFSR) that processes the cipher's parameterizing key consists of two parts, of lengths t and r. Like a usual execution of a long input hash transformation, the process consists of consecutive iterations. The number of iterations is the number of t-bit blocks of which the input data consists. (Possible padding may take place, to make the length of the input data a multiple of t.)

Being able to perform a hashing H on chained input blocks, an HMAC is implemented as HMAC(text,K)=H[Kout‖H(Kin‖text)]

Security Considerations and Requested Features of the Stream Cipher

1) Considerations per Iteration

Each iteration in the described process performs a one-way block transformation on a ðr þ tÞ-bits block. This applies to the irreversibility of the transformation; the strong dependence on each input bit; randomness of the output; balanced mapping; correlation attack; and collision attack.

2) Considering the Transition from a Single-Block Transformation to Sequential Processing

The transition from the structure depicted in Fig. 2 to that of Fig. 3 has its own security implications. Even if the stream cipher facilitates a strong one-way block transformation, the cipher should also provide for secured iterative implementation. In this respect, there is a need for an available well analyzed stream cipher which is based on having an initializing nonsecret value being a part of the parameterizing key.

CONCLUSION

RFID and Wireless Sensor Networks pose a need for efficient implementation of MAC. To achieve efficiency, while not sacrificing security, there is a need to evaluate new approaches, while also utilizing any characteristic of the specific implementation of MAC that can enhance efficiency. A complete highly compact MAC implementation, based on stream ciphering, was presented.

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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] Dr.AntoBennet, M., Karthika, S., Durga Devi, A., Lakshmisree, B., & Thilagavathi, S.(2016). Implementation of Portable Fetal and Maternal Heart Rate Recorder by Using RISC Microcontroller. *Excel International Journal of Technology, Engineering and Management, 3*(2), 58-61.

[16] Gokila, L., Poongodi, V., and Dr.Thangadurai, K. (2016). Multi Scheduling Reactive Resource Sharing for Dynamic Dataflow in Cloud Environment. *Bonfring International Journal of Data Mining, 6*(4), 46-52.

[17] Orhorhoro, E.K., Orhorhoro, O.W., & Ogini, M.E. (2016). Assembly and Investigation of Solar Powered Air Conditioner for Household Use in Nigeria. *International Academic Journal of Innovative Research, 3*(10), 84-99.

[18] Prabha, I.M.T., & Gayathri, R. (2014). Isolation Enhancement in Microstrip Antenna Arrays. *International Journal of Communication and Computer Technologies, 2*(2), 79-84.

[19] Jamuna, K., Jayapriya, G., & Jayanthi, K. (2014). Mems Based Haptic Assistive System for Physical Impairments. *International Journal of Communication and Computer Technologies, 2*(2), 88-93.

[20] Bourvil, & Levi. (2017). Multi-Level Trust Privacy Preserving Data Mining to Enhance Data Security and Prevent Leakage of the Sensitive Data. *Bonfring International Journal of Industrial Engineering and Management Science, 7*(2), 21-25.

[21] Mozaffari, M., Pourbahram, A., & Marzdashti, A.F. (2015). Knowing Effective Factors in Reducing Power Consumption in MAC Protocols' Listening For Wireless Sensor Networks. *International Academic Journal of Science and Engineering, 2*(5), 14-21.

[22] Youzband, R.S., & Mirnia, M.K. (2015). Designing Reverse Converter for the New Three-Moduli Set {2^(2n+1), 2^n-1, 2^n+1}. *International Academic Journal of Science and Engineering, 2*(5), 32-38.

[23] Rajalakshmi, M., & Subadra, S. (2014). Smile Emotional Identification for Negative Emotions Detection by Fuzzy Neural Network with Pixel Differences. *International Journal of System Design and Information Processing, 2*(4), 59-65.

[24] Gopalakrishnan, C., & Iyapparaja, M. (2018). Tagging in IoT Category based Applications Using Vitality Proficient Geospatial Technique. *Bonfring International Journal of Networking Technologies and Applications, 5*(2), 1-5.

[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.