Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2017 12 (4): 118-124

Security and Privacy in Distributed Systems through Multifactor Authentication

G. Michael, R. Kavitha

Received: 06 December 2016 ▪ Revised: 09 January 2017 ▪ Accepted: 08 February 2017

Abstract: Based on security in distributed systems different resources need security from unknown persons. This paper provides approach for authenticate clients by four factors namely password, smartcard, fingerprint and sms. Here in this paper it is proposed to develop three factor to four factor authentication. Here in this fuzzy logic concept is used to provide better security. By this fuzzy logic, if there is any mismatch or suspicious in fingerprint the server will send one time password to the user mobile and to improve privacy security questions are asked.

Keywords: Authentication, Distributed Systems, Security, Password, Smart Card, Fingerprint, SMS.

INTRODUCTION

In this distributed system, different resources are managed by servers. The four authentication factors are, Password, Smartcard, Fingerprint, sms. Multi-factor authentication is as an approach to security authentication, which requires that the user of a system provide more than one form of verification in order to prove their identity and allow access to the system. Multi-factor authentication takes advantage of a combination of several factors of authentication; three major factors include verification by something a user knows (such as a password), something the user has (such as a smart card), and something the user is (such as the use of biometrics). Due to their increased complexity, authentication systems using a multi-factor configuration are harder to compromise than ones using a single factors. Security issues in distributed systems and network systems are extremely important. Almost all modern applications need, in one way or another, to encrypt their users' passwords. We could say that, from the moment that an application has users, and users sign in using a password, these passwords have to be stored in an encrypted way.

There are some intuitive reasons for this: our data stores can be compromised, and so can our communications. But the most important reason is that we have to think of our users' passwords as sensitive personal data. Their passwords are their key to their privacy, so they are personal, they are sensitive, and no one (not even us) has the right to know them. And we must honor this if we want to gain our user's trust. One of the most important security features used today are passwords. It is important for both you and all your users to have secure, un guessable passwords.

It's common understanding these days that the more factors of identification that a user has to provide to an authentication system, the more trustworthy and secure it likely is. Single-factor authentication is usually accomplished by providing *something you know,* like a password or PIN number. As two-factor authentication became more and more mainstream, the two factors involved have usually been *something you know*, and *something you have,* like a credit card, crypto-key USB device, a code generated every so often by a electronic card you keep in your wallet, a smart-card that can respond directly to cryptographic challenges, or an RFID or other radio device. The most common use of two-factor authentication is how bank customers authenticate to an ATM machine; they must provide *something they have*, their bank card, and *something they know*, it's PIN.

Fingerprint are the most widely used biometric feature for person identification and verification in the field of biometric identification. Biometric authentication consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control.

G. Michael, Associate Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: michaelcse@gmail.com

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

It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to identify individualsA form of knowledge representation suitable for notions that cannot be defined precisely, but which depend upon their contexts.

Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. In contrast with traditional logic theory, where binary sets have two-valued logic: true or false, fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false. Furthermore, when linguistic variables are used, these degrees may be managed by specific functions. Fuzzy logic provides an alternative way to represent linguistic and subjective attributes of the real world in computing.

A distributed system consists of a collection of autonomous computers, connected through a network and distribution middleware, which enables computers to coordinate their activities and to share the resources of the system, so that users perceive the system as a single, integrated computing facility.

A. Characteristics of Distributed Systems

1. Components are not shared by all users.
2. Resources may not be accessible.
3. Software runs in concurrent processes on different processors.
4. Multiple Points of control
5. Openness.
6. Scalability.
7. Fault Tolerance.

RELATED WORK

User authentication is the process of verifying whether the identity of a user is genuine prior to granting him access to resources or services in a secured environment. Traditionally authentication is performed statically at the point of entry of the system (e.g. login); this is referred to as static authentication. A popular form of a static authentication technique widely used in computer networks is password-based authentication. It is a well-established fact that traditional passwords are unsafe. Passwords may be stolen or may be cracked using the so-called dictionary attack. Generally speaking there are at least two main issues with static authentication techniques.

Firstly, in the case where the authentication process fails to genuinely verify the identity of a user as may happen, for instance, with password-based authentication schemes there is no other opportunity to get things right in the rest of the login session or to establish after the session that some malicious activity occurred. Secondly, a successful authentication at the beginning of a session does not provide any remedy against the session being hijacked later by some malicious user.

One of the solutions proposed to address these shortcomings is continuous authentication (CA). CA consists of the process of positively verifying the identity of a user in a repeated manner throughout a login session. CA departs from the traditional (static) authentication schemes by repeating several times the authentication process dynamically throughout the entire login session; the main objectives being to detect masqueraders, ensure session security, and combat insider threat.

Although CA can be effective in detecting session hijacking, it requires special data sources to detect masqueraders. Such data source should allow the system to discriminate reliably legal users from imposters. Although non-biometric data sources such as user commands sequences and RFID may be used, biometrics technologies are the most suitable for this purpose.

One-factor authentication – this is “something a user knows.” The most recognized type of one-factor authentication method is the password. Two-factor authentication – in addition to the first factor, the second factor is “something a user has.” Examples of something a user has are a fob that generates a pre-determined code, a signed digital certificate or even a biometric such as a fingerprint. The most recognized form of two-factor authentication is the ubiquitous RSA SecurID fob.

Three-factor authentication in addition to the previous two factors, the third factor is “something a user is.” Examples of a third factor are all biometric such as the user’s voice, hand configuration, a fingerprint, a retina scan or similar. The most recognized form of three-factor authentication is usually the fingerprint.

Recent years have seen an increasing interest in biometric systems; the underlying technology has improved and the costs involved have been reduced considerably. Biometrics technologies are widely used in various security applications, and are considered among the most accurate and efficient security systems on the market. Biometrics can be defined as a set of distinctive, permanent and universal features recognized from human physiological or behavioral characteristics.

Such use of two of the same factors is considered multi-factor authentication and is not related to any of the aforementioned definitions. So those of you that are using two different user identifiers and passwords are not using two-factor authentication, you are using multi-factor authentication.

Biometric Recognition Process

Biometric recognition involves comparing an enrolled biometric sample (biometric template)against a newly captured biometric sample (for example, finger scan provided at an access at-tempt). A three-step process (Acquire, Process, and Store) should be executed every time the user presents his or her biometric sample to the system as follows:

1. Acquire: Raw biometric data is acquired by a sensing device, such as the image produced by a fingerprint scanning device, or the data collected by a keystroke event logger. Raw biometric data usually contains noise and cannot be used as is to automatically compare between users.
2. Process: The raw data is processed to build a biometric model (template). This model consists of a number of extracted distinguishing features which are represented in a mathematical format.
3. Store: The biometric template is stored in a database with all other collected information, (like claimed identity, date, time). This process is required in order to secure enough data for the user enrollment process. Some of the biometric systems implementations do not permanently store the generated template during the recognition process.

This is usually the case for non-audited access control systems. However storing such data increases the accountability of the system. Since the biometric template contains all the data representing the user biometric characteristics to the system there is no need to store the raw data. It is also not possible to reconstruct the raw data from the generated biometric template.

PROPOSED WORK

In this proposed system fuzzy logic concept is used. By this if there is any mismatch in fingerprint server will send one time password to user mobile. In this if there is invalid password anr rfid means it wont give permission to access. In this if the fingerprint matching ranges above 80% means we can directly access the banking transactions. If the fingerprint range is above 70% to 80% means server will send one time password. If the range is below 70% means invalid fingerprint. Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. In contrast with traditional logic theory, where binary sets have two-valued logic: true or false, fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false.

One time password generated by the server will be a random number generation. By this user can enter one time password to log on in to the banking system. By this it can provide better security.

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that, if a potential intruder manages to record an OTP that was already used to log into a service or to conduct a transaction, he or she will not be able to abuse it since it will be no longer valid. Unlike a static password, a one-time password changes each time the user logs in. The passwords themselves are generated in one of two ways: either as time-synchronized or counter-synchronized. Challenge-based OTPs are a special case and also often use a hardware device. However, the user must provide a known value, such as a personal identification number (PIN), to cause the OTP to be generated. By this one time password will provide better security.

For providing better security security question and answer will be registered during admin registration. If the fingerprint match score is above 90% means we can easily access banking transaction. If the score range is 80% to 90% means security question will be asked, if answered correctly means we can perform banking transaction, otherwise we cant access. If the score range is below 80% means invalid fingerprint message is obtained, therefore he cant perform the transaction.

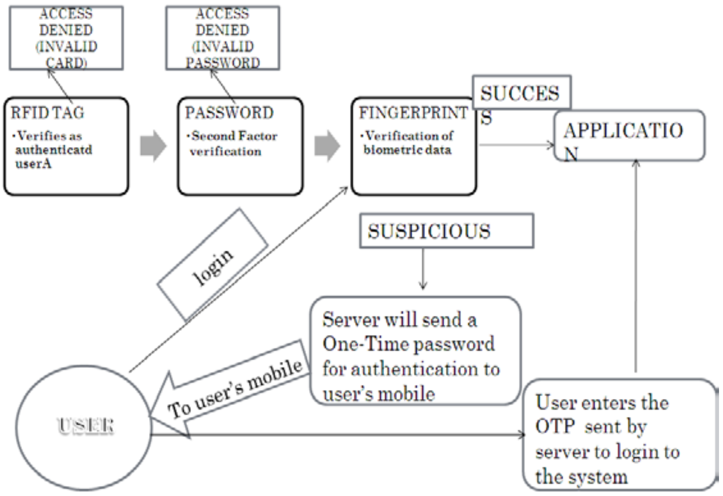
ACCESS DENIED (INVALID CARD)
ACCESS DENIED (INVALID PASSWORD
RFID TAG
•Verifies as authenticatd userA
PASSWORD
•Second Factor verification
FINGERPRINT
•Verification of biometric data
SUCCES S
APPLICATIO N
SUSPICIOUS
login
Server will send a One-Time password for authentication to user's mobile
To user's mobile
User enters the OTP sent by server to login to the system
USER

Fig. 1: Architecture of proposed system

Client

User will be registering the Server, by giving their Name, Phone Numbers, E mail ID, Address & other particulars during registering phase. Along with he has to register RFID, Finger print and Key pad value. These details should be stored in the main server.

Server

In this module the server stores all the required information for further precedence. The server acts a main database to all the clients when the authentication is needed and further it can act a storage system of entire project. The server is responsible for maintain all the authentication information about all the client who are all register before.

RFID

User will retrieve the data stored in the data server by giving the pass key along with the RFID Authentication. While voting, the user should swipe the RFID card in the polling system. Then the system compares the given RFID Number with the server's RFID number. When the user login to the merchant website he has to enter his secret pin number via the keypad matrix. Because keypad matrix has its own unique id and some separate format. When the user enters the number in keypad matrix the pin number along with the corresponding keypad id also transferred to the bank server.

Finger Print with Fuzzy Logic

To provide more security the customer has to give his finger print along with the other login information. Finger print of the particular bank client is already stored in the server's database. If the given fingerprint matches with the existing database then only he can precede the transaction Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false.

Algorithm 1: RSA

```
Step1: Select random prime numbers $p$ and $q$, and check that $p != q$
Step2: Compute modulus $n = pq$
Step3: Compute phi, $ø= (p - 1)(q - 1)$
Step4: Select public exponent $e$, $1 < e < ø$such that $gcd(e,ø)=1$
Step5: Compute private exponent $d = e - 1 \bmod ø$
Step6: Public key is $\{n, e\}$, private key is $d$
```

Algorithm 1: Minitiae

```
Step1: Consider the 256*256 array
Step 2: Scan the image from top to bottom, left to right order by following only ridges
Step 3: Find the 0-1 transition, calculate the width of theridge by noting the 1-0 transition
Step 4: Move to the next row and follow the same ridge Note the width
Step 5: If the width >=width in previous row there may be a top to bottom bifurcation .Call the bifurcation function to check if it is a minutiae point
Else
```

If the width =< width in previous row there may be a bottom to p ridge bifurcation. Call the bifurcation function to check if it is a minutiae Point

- Step 6: Continue with the next row and repeat this for all theirdges in the given image or until 90 minutiae points have been obtained.

IMPLEMENTATION

The implementation has been done with the help of above architecture diagram .All experiments are done on an intel Pentium dual core processor, with 2GB RAM and 160GB hard disk. In the software requirements wise windows XP operating system has been used. For front end designing purpose Java Jdk1.5, and for back end data storage purpose SQL server 2005 has been used. For RSA algorithm and Minituia algorithm, In this implementation we have succeeded with the all the modules.

CONCLUSION

Preserving security and privacy is a challenging issue in distributed systems. This paper makes a step forward in solving this issue by proposing a four-factor authentication to protect services and resources from unauthorized use. The authentication is based on password, smart card, and biometrics and sms. Here in this fuzzy logic concept is used. By this if there is any mismatch in fingerprint one time password will be sent by the server to the user mobile.

REFERENCES

[1] Das, J., Das, M. P., & Velusamy, P. (2013). Sesbania grandiflora leaf extract mediated green synthesis of antibacterial silver nanoparticles against selected human pathogens. *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, *104*, 265-270.

[2] Umanath, K.P.S.S.K., Palanikumar, K., & Selvamani, S. T. (2013). Analysis of dry sliding wear behaviour of Al6061/SiC/Al2O3 hybrid metal matrix composites. *Composites Part B: Engineering*, *53*, 159-168.

[3] Udayakumar, R., Khanaa, V., Saravanan, T., & Saritha, G. (1786). Cross layer optimization for wireless network (WIMAX). *Middle-East Journal of Scientific Research*, *16*(12), 1786-1789.

[4] Kumaravel, A., & Rangarajan, K. (2013). Algorithm for automaton specification for exploring dynamic labyrinths. *Indian Journal of Science and Technology*, *6*(5S), 4554-4559.

[5] Pieger, S., Salman, A., & Bidra, A.S. (2014). Clinical outcomes of lithium disilicate single crowns and partial fixed dental prostheses: a systematic review. *The Journal of prosthetic dentistry*, *112*(1), 22-30.

[6] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum. *Colloids and Surfaces B: Biointerfaces*, *94*, 114-117.

[7] Khanaa, V., Mohanta, K., & Satheesh, B. (2013). Comparative study of uwb communications over fiber using direct and external modulations. *Indian Journal of Science and Technology*, *6*(6), 4845-4847.

[8] Zain, Z. (2019). High Speed and Low Power GDI based Full Adder. *Journal of VLSI Circuits and Systems, 1*(1), 5-9.

[9] Udupa, P., & Vishwakarma, S. (2016). A Survey of MRI Segmentation Techniques for Brain Tumor Studies. *Bonfring International Journal of Advances in Image Processing, 6*(3), 22-27.

[10] Jacob, L., & Quinn, S. (2018). Finding of Frequent Itemset with Two Mask Searches. *Journal of Computational Information Systems, 14*(2), 36-43.

[11] Manjula, S., & Dr. Banu, R., (2014).An Efficient Compound Scoring Gene Selection Technique (CSGS) for Cancer Classification using Microarrays. *International Journal of Advances in Engineering and Emerging Technology, 5*(5), 234-247.

[12] Saravanan, G., and Dr.Gopalakrishnan, V. (2014). Resource Allocation for Multimedia Communication on Grid Computing Environment using Hybrid ABC. *Excel International Journal of Technology, Engineering and Management, 1*(2), 36-41.

[13] Dr. John, E.T., Skaria, B., & Shajan, P.X. (2016). An Overview of Web Content Mining Tools. *Bonfring International Journal of Data Mining, 6*(1), 01-03.

[14] Alviri, F., & Habibi, S.F. (2015). Reviewing Self-Adaptation Frameworks for the Implementation of Enterprise Resource Planning Systems. *International Academic Journal of Innovative Research, 2*(4), 1-10.

[15] Soni, K., Kumar, U., & Dosodia, P. (2014). A Various Biometric Application for Authentication and Identification. *International Journal of Communication and Computer Technologies, 2*(1), 6-10.

[16] Dr.Sebasthirani, K., and Mahalingam, G. (2018). Design of Shunt Active Power Filter with Fuzzy Logic Control for Mitigating Harmonics. *Bonfring International Journal of Industrial Engineering and Management Science, 8*(2), 26-30.

[17] Asgarnezhad, R., & Mohebbi, K. (2015). A Comparative Classification of Approaches and Applications in Opinion Mining. *International Academic Journal of Science and Engineering, 2*(5), 1-13.

[18] Khanaa, V., Thooyamani, K. P., & Udayakumar, R. (1798). Cognitive radio based network for ISM band real time embedded system. *Middle-East Journal of Scientific Research*, *16*(12), 1798-1800.

[19] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum. *Materials Letters*, *75*, 33-35

[20] Caroline, M.L., Sankar, R., Indirani, R.M., & Vasudevan, S. (2009). Growth, optical, thermal and dielectric studies of an amino acid organic nonlinear optical material: l-Alanine. *Materials Chemistry and Physics*, *114*(1), 490-494.

[21] Kumaravel, A., & Pradeepa, R. (2013). Efficient molecule reduction for drug design by intelligent search methods. *International Journal of Pharma and Bio Sciences*, *4*(2), B1023-B1029.

[22] Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., Ladchumananandasiivam, R., De Gomes, U. U., & Maaza, M. (2016). Synthesis and characterization studies of NiO nanorods for enhancing solar cell efficiency using photon upconversion materials. *Ceramics International*, *42*(7), 8385-8394.

[23] Sengottuvel, P., Satishkumar, S., & Dinakaran, D. (2013). Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling. *Procedia Engineering*, *64*, 1069-1078.

[24] Anbuselvi S., Chellaram, C., Jonesh S., Jayanthi L., & Edward J.K.P. (2009). Bioactive potential of coral associated gastropod, Trochus tentorium of Gulf of Mannar, Southeastern India. *J. Med. Sci,* 9(5), 240-244.

[25] Kaviyarasu, K., Ayeshamariam, A., Manikandan, E., Kennedy, J., Ladchumananandasivam, R., Gomes, U. U., & Maaza, M. (2016). Solution processing of CuSe quantum dots: Photocatalytic activity under RhB for UV and visible-light solar irradiation. *Materials Science and Engineering: B*, *210*, 1-9.

[26] Kumaravel, A., & Udayakumar, R. (2013). Web portal visits patterns predicted by intuitionistic fuzzy approach. *Indian Journal of Science and Technology*, *6*(5S), 4549-4553.

[27] Srinivasan, V., & Saravanan, T. (2013). Reformation and market design of power sector. *Middle-East Journal of Scientific Research*, *16*(12), 1763-1767.

[28] Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2015). A comparative study on the morphological features of highly ordered MgO: AgO nanocube arrays prepared via a hydrothermal method. *RSC Advances*, *5*(100), 82421-82428.

[29] Kumaravel, A., & Udhayakumarapandian, D. (2013). Consruction of meta classifiers for apple scab infections. *International Journal of Pharma and Bio Sciences*, *4*(4), B1207-B1213.

[30] Sankari, S. L., Masthan, K. M. K., Babu, N. A., Bhattacharjee, T., & Elumalai, M. (2012). Apoptosis in cancer-an update. *Asian Pacific journal of cancer prevention*, *13*(10), 4873-4878

[31] Harish, B. N., & Menezes, G. A. (2011). Antimicrobial resistance in typhoidal salmonellae. *Indian journal of medical microbiology*, *29*(3), 223-229.

[32] Manikandan, A., Manikandan, E., Meenatchi, B., Vadivel, S., Jaganathan, S. K., Ladchumananandasivam, R., & Aanand, J. S. (2017). Rare earth element (REE) lanthanum doped zinc oxide (La: ZnO) nanomaterials: synthesis structural optical and antibacterial studies. *Journal of Alloys and Compounds*, *723*, 1155-1161.

[33] Caroline, M. L., & Vasudevan, S. (2008). Growth and characterization of an organic nonlinear optical material: L-alanine alaninium nitrate. *Materials Letters*, *62*(15), 2245-2248.

[34] Saravanan T., Srinivasan V., Udayakumar R. (2013). A approach for visualization of atherosclerosis in coronary artery, Middle - East Journal of Scientific Research, 18(12), 1713-1717.

[35] Poongothai, S., Ilavarasan, R., & Karrunakaran, C.M. (2010). Simultaneous and accurate determination of vitamins B1, B6, B12 and alpha-lipoic acid in multivitamin capsule by reverse-

phase high performance liquid chromatographic method. *International Journal of Pharmacy and Pharmaceutical Sciences*, *2*(4), 133-139.

[36] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Synthesis and structural characterization of thin films of SnO 2 prepared by spray pyrolysis technique. *Indian Journal of Science and Technology*, *6*(6), 4754-4757

[37] Anbazhagan, R., Satheesh, B., & Gopalakrishnan, K. (2013). Mathematical modeling and simulation of modern cars in the role of stability analysis. *Indian Journal of Science and Technology*, *6*(5S), 4633-4641.

[38] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of bis thiourea cadmium iodide: A semiorganic single crystal. *Materials Chemistry and Physics*, *113*(2-3), 670-674.

[39] Sharmila, S., Jeyanthi Rebecca, L., & Das, M. P. (2012). Production of Biodiesel from Chaetomorpha antennina and Gracilaria corticata. *Journal of Chemical and Pharmaceutical Research*, *4*(11), 4870-4874.

[40] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2013). An integrated agent system for e-mail coordination using jade. *Indian Journal of Science and Technology*, *6*(6), 4758-4761.

[41] Caroline, M. L., Kandasamy, A., Mohan, R., & Vasudevan, S. (2009). Growth and characterization of dichlorobis l-proline Zn (II): A semiorganic nonlinear optical single crystal. *Journal of Crystal Growth*, *311*(4), 1161-1165.

[42] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of L-phenylalanine nitric acid, a new organic nonlinear optical material. *Materials Letters*, *63*(1), 41-44.

[43] Kaviyarasu, K., Xolile Fuku, Genene T. Mola, E. Manikandan, J. Kennedy, and M. Maaza. Photoluminescence of well-aligned ZnO doped CeO2 nanoplatelets by a solvothermal route. *Materials Letters*, *183*(2016), 351-354.

[44] Saravanan, T., & Saritha, G. (2013). Buck converter with a variable number of predictive current distributing method. *Indian Journal of Science and Technology*, *6*(5S), 4583-4588.

[45] Parthasarathy, R., Ilavarasan, R., & Karrunakaran, C. M. (2009). Antidiabetic activity of Thespesia Populnea bark and leaf extract against streptozotocin induced diabetic rats. *International Journal of PharmTech Research*, *1*(4), 1069-1072.

[46] Hanirex, D. K., & Kaliyamurthie, K. P. (2013). Multi-classification approach for detecting thyroid attacks. *International Journal of Pharma and Bio Sciences,* 4(3), B1246-B1251

[47] Kandasamy, A., Mohan, R., Lydia Caroline, M., & Vasudevan, S. (2008). Nucleation kinetics, growth, solubility and dielectric studies of L-proline cadmium chloride monohydrate semi organic nonlinear optical single crystal. *Crystal Research and Technology: Journal of Experimental and Industrial Crystallography*, *43*(2), 186-192.

[48] Srinivasan, V., Saravanan, T., Udayakumar, R., & Saritha, G. (2013). Specific absorption rate in the cell phone user's head. *Middle-East Journal of Scientific Research*, *16*(12), 1748-50.

[49] Udayakumar R., Khanaa V., & Saravanan T. (2013). Chromatic dispersion compensation in optical fiber communication system and its simulation, Indian Journal of Science and Technology, 6(6), 4762-4766.

[50] Vijayaragavan, S.P., Karthik, B., Kiran, T.V.U., & Sundar Raj, M. (1990). Robotic surveillance for patient care in hospitals. *Middle-East Journal of Scientific Research*, *16*(12), 1820-1824.