Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2017 12 (4): 35-43

Secure and Efficient Way of Handling Medical Records in Cloud

R. Elankavi, Dr.R. Udayakumar

Received: 02 December 2016 ▪ Revised: 05 January 2017 ▪ Accepted: 04 February 2017

Abstract: Personal health records (PHRs) are touted as a new convenience technology for consumers. It enables the patients to create a health information of their own in a centralized way, which alleviate the storage, access and sharing of health data in the cloud environment. By storing the health information in the cloud various security issues should arise such us authorization, key management and efficient user revocation, therefore, before outsourcing the PHR in the cloud, it is a promising method to encrypt the PHR using Attribute Based Encryption. Existing cryptographic schemes are planned for single owner settings, here, dealt with multiple owner scenarios which reduce the key management complexity for owners and users. Enhancing the MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. The experimental results will show the security and efficiency of the proposed system.

Keywords: Virtualization, Personal Health Record, HealthCare Social Network, Attribute Based Encryption.

INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing [1] of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends.

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing [1] of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. A feasible and promising approach would be to encrypt [3] the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access [2] to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users.

BACKGROUND

Types of Cloud

There are four main type of cloud:

1. **Public cloud**: The Cloud computing resource is shared outside, anyone can use it and some payment maybe need.
2. **Private cloud**: It is opposite to public cloud, private cloud's resource is limit to a group of people, like a staff of a company etc.
3. **Hybrid cloud**: this is a mixture of previous two clouds, some cloud computing resource is shared outside but some don't.

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

Dr.R. Udayakumar, Professor, Department of IT, BIST, BIHER, Bharath Institute of Higher, Education & Research, Selaiyur, Chennai. E-mail: rsukumar2007@gmail.com

4. **Community cloud**: this is a special cloud to make use of cloud computing features. More than one community shares a cloud to share and reduce the cost of computing system.

Virtualization

Virtualization technology lets a single PC or server simultaneously run multiple operating systems or multiple sessions of a single OS. This lets users put numerous applications even those that run on different operating systems on a single PC or server instead of having to host them on separate machines as in the past. The approach is thus becoming a common way for businesses and individuals to optimize their hardware usage by maximizing the number and kinds of jobs a single CPU can handle.

Cryptographic Technique

Attribute-based Encryption

It is a type of public key Encryption, in which the secret key of a user and the cipher text are dependent about attributes. In a such as a System the decryption [4] of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

Multi-Authority Attribute Based Encryption

In a desired Multi-Authority CP-ABE (MA-CP-ABE) [4] system, different domains of attributes are managed by different authorities. An encrypt or can encrypt messages with any access policy over the entire attribute universe.

Key-Policy Attribute based Encryption

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE [7] data are associated with attributes for each of which a public key component is defined. The encrypt are associates the set of attributes to the message by encrypting it with the corresponding public key components.

Ciphertext-Policy Attribute based Encryption

CP-ABE is a tool for implementing fine-grained access control [8] over encrypted data, and is conceptually similar to traditional access control methods such as Role-Based Access Control [21].

RELATED WORKS

In the past, health care providers (such as the family doctor) have stored medical records of their patients on paper locally. This allowed a controlled environment with easy management of data privacy and security: keeping the paper records in a locked cabin at the doctor's practice. Even the increasing use of personal computers and modern information technology in medical institutions allowed for a moderate effort to manage privacy and confidentiality of individual medical records. This was due to the decentralized and locally managed infrastructure of each institution. But nowadays outsourcing [6] of IT infrastructure (e.g., cloud computing) and other services (e.g., billing processing and accounting for medical practices) leads to a complex system where privacy-sensitive data are stored and processed at many different places. Hence, it becomes attractive to store and process healthcare data in the cloud (at outsourced data providers that can be accessed via the Internet). While such e-health systems promise a more cost-efficient service and improved service quality, the complexity to manage data security and privacy increases, too.

In existing system, the PHRs are stored on a server of a third party in the cloud. The PHR server provider is responsible for ensuring data protection. Typically, patients can define role-based access rights [3] for individual health professionals.

For example, they can define full access to their family doctor, but only restricted access to some data to their fitness trainer or health coach. The advantages of such an approach are that the PHR is accessible from everywhere because of the centralized management [10] (IT outsourcing). The patient can easily give one doctor access to data and test results that were determined by another doctor, when the data is stored in the PHR. This can help to avoid double examination. Moreover, due to the individual management of PHRs by the patients, it is expected that people are more aware of their own health. This could reduce the healthcare costs in the long term as well. However, from a technical perspective this model has a great disadvantage regarding patients' privacy. On the one hand, patients need to manage complex access rights and need to understand their implications. On the other hand, they need to rely on the robustness and correctness of the security mechanisms implemented at the PHR server provider. In general, it may be possible for the server provider to gain access to the data stored in PHRs.

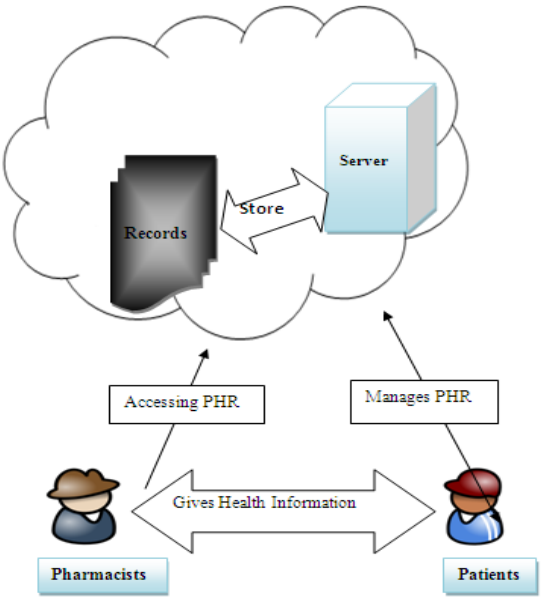

Figure 1: Existing System

PROPOSED WORKS

Considerations

Personal health record is an model for exchanging the health information which is outsourced to be stored at a third party, such as cloud providers. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. A feasible and promising approach would be to encrypt the data before outsourcing [20]. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. The proposed framework describes patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file.

Architecture

Patient Centric Framework

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD [5] can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner. Which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. Role attributes are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs [19], without directly interacting with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies for her PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users [11], it greatly reduces the key management overhead for both the owners and users.

Key Distribution- PHR Encryption and Access

Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN) [12] (which could be part of the PHR service. There are two ways for distributing secret keys [9]. First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access), and the owner will grant

her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs key gen [15] of KP-ABE to generate the user secret key that embeds her access structure. In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation, when the user is granted all the file types under a category, her access privilege will be represented by that category instead. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files [13], excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root. The data readers download PHR files from the server, and they can decrypt the files only if they have suitable attribute based keys. The data contributors will be granted write access to someone's PHR, if they present proper write keys.

ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained [14] access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems [18], where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) [16] to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs,

1. Stores data in Cloud.
2. Get Attributes.
3. Write Access.
4. Revoke.

which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

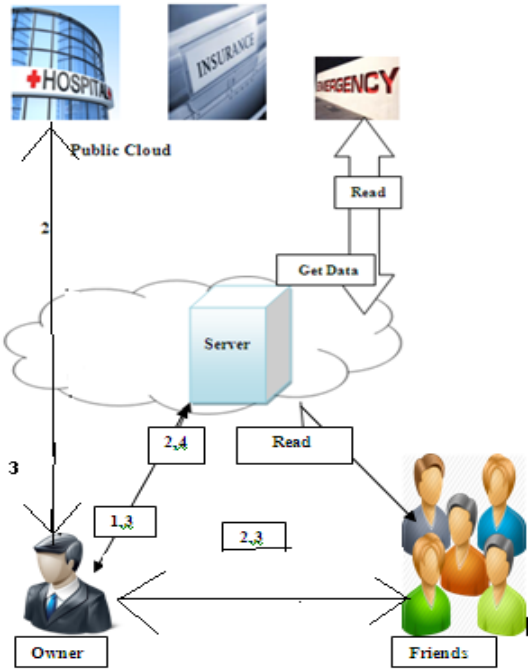

Figure 2: Proposed System

Break-glass Module

In this module when an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department ED to prevent from abuse of Break-glass option, the emergency staff needs to contact the ED to verify her Identity and the emergency situation, and obtain temporary read keys [17]. After the Emergency is over; the patient can revoke the emergent access via the ED.

Technical Layout

Introducing Web Application

Organizations are increasingly becoming dependent on the Internet for sharing and accessing information. This Internet boom has changed the focus of application development from stand-alone applications to distributed Web applications. Web applications are programs that can be executed either on a web server or in a web browser. They enable you to share and access information over the Internet and operate intranets.

Introduction to ASP.NET

ASP.NET is a part of the .NET Framework, a new computing platform from Microsoft optimized for creating applications that are highly distributed across the Internet. Highly distributed, here means that the components of the applications, as well as the data, may reside anywhere in the Internet rather than all being contained inside one software program somewhere. It is a programming framework, and one of the primary differences between it and traditional ASP is that it uses a common language runtime (CLR) capable of running compiled code on a web server to deploy powerful wed-based applications.

ASP.NET still use HTTP to communicate to the browser and back, but it brings added functionality that makes the communication process much richer. If any files have the appropriate extension or contain code, the server routes those files to ASP.NET for processing prior to sending them out to the client. The script or code is then processed and the appropriate content is generated for transmission back to the browser/client.

Because processing takes place before the results are delivered to the user, all manner of functionality can be built-in such as database access, component usage and the ordinary programmatic functionality available with scripting languages. Microsoft has introduced ASP. ASP.NET is the .NET version of ASP. ASP.NET is a standard HTML file that contains embedded server-side scripts.

ASP.NET in .NET Framework

ASP.NET, which is the .NET version of ASP, is built on Microsoft .NET Framework. Microsoft introduced the .NET Framework to help developers create globally distributed software with Internet functionality and interoperability. The elements of an ASP.NET application include Web service to provide a mechanism for programs to communicate over the Internet.

ADO.NET

ADO.NET is all about data access. Data is generally stored in a relational database in the form of related tables. Retrieving and manipulating data directly from a database requires the knowledge of database commands to access the data.

Results

The Screen Shots of our project is captured and listed below.

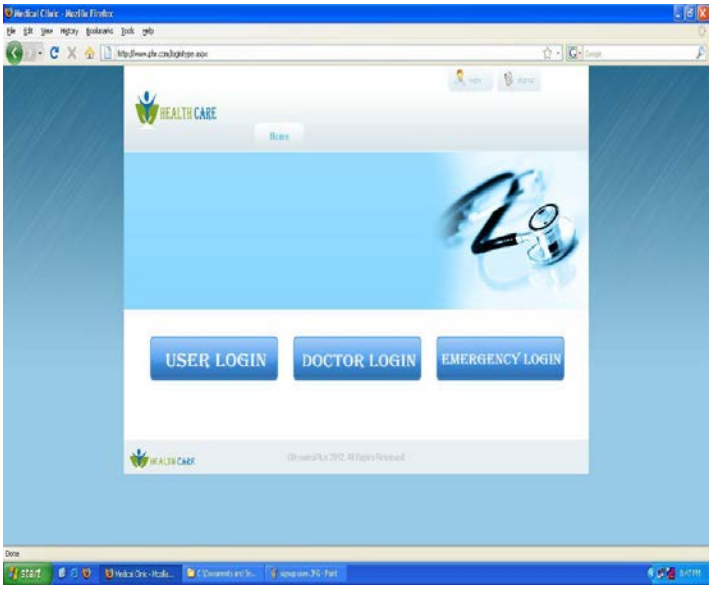

Fig. 3: Various Login Form

Fig. 4: Adding medical Detail

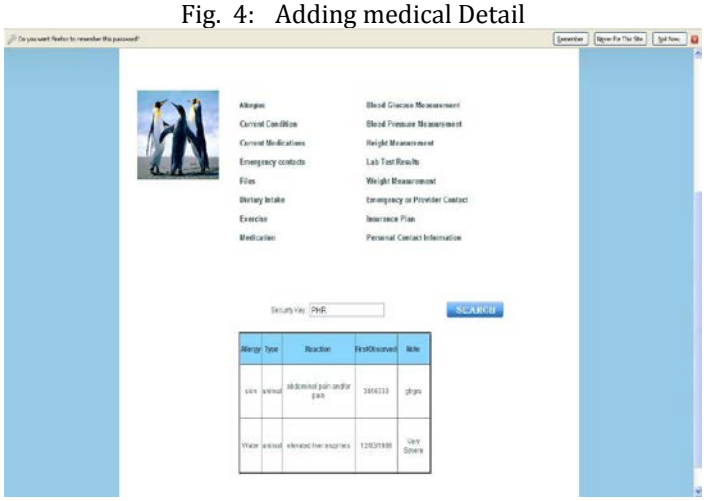

Fig. 5: A doctor viewing a patient's information

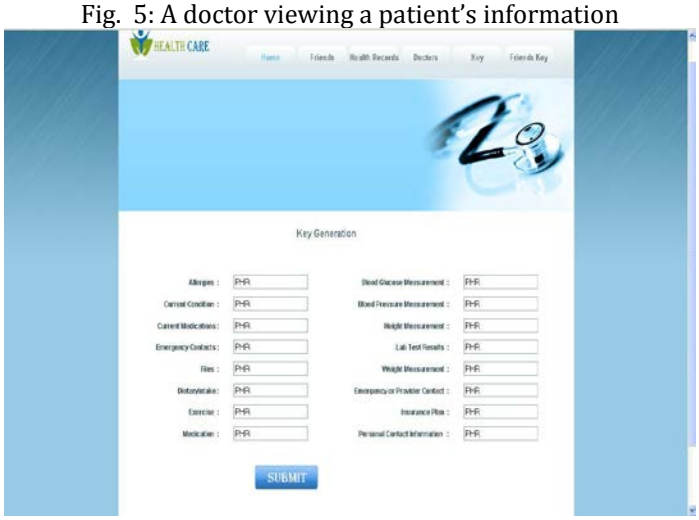

Fig. 6: Key Generation

CONCLUSION AND FUTURE ENHANCEMENTS

Conclusions

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security.

Future Enhancements

As future study, it will be interesting to enhance the HSN with a third party auditor to verify the cloud server that stores and process the PHRs. Homomorphic Split key Encryption can become additional enhancement to verify the trustworthiness of the TPA.

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] Gokula Krishnan, C.A., & Dr. Suphalakshmi, A. (2017). An Improved MAC Address Based Intrusion Detection and Prevention System in MANET Sybil Attacks. *Bonfring International Journal of Research in Communication Engineering, 7*(1), 1-5.

[9] Kurian, S., & Franklin, R.G. (2013). Trustworthy Coordination of Web Services Atomic Transaction for Net Banking. *The SIJ Transactions on Advances in Space Research & Earth Exploration, 1*(1), 6-9.

[10] Dr.Gopinath, B., Kalyanasundaram, M., Karthika, V., & Pradeepa, M. (2018). Development of Power Quality Event Using Diode Clamped Multilevel Inverter in Conjunction with AANF. *Bonfring International Journal of Software Engineering and Soft Computing, 8*(1), 17-22.

[11] 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.

[12] 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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] Dr. Chaturvedi, A., Bhat, T.A., & Kumar, V. (2013). Movement based Asynchronous Recovery System in Mobile Computing System. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 1*(3), 1-5.

[21] Jerin Jose, M., Akmal Jahan, S., Arunachalam, R., Karnan, R., & Kishore, V. (2017). Automobile Accident Sensing Unit and Notifier using Arduino. *The SIJ Transactions on Industrial, Financial & Business Management (IFBM), 5*(1), 5-8.

[22] Hoa, N.T., & Voznak, M. (2019). High Speed and Reliable Double Edge Triggered D- Flip-Flop for Memory Applications. *Journal of VLSI Circuits and Systems*, *1*(1), 13-17.

[23] Shamim, F.M., & Vishwakarma, S. (2016). Exploiting the Motion Learning Paradigm for Recognizing Human Actions. *Bonfring International Journal of Advances in Image Processing, 6*(3), 11-16.

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

[25] 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.

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

[27] 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

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

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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

[34] 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.

[35] 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.

[36] 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.

[37] Kumar, K.A., Sadulla, S., & A. Surendar, (2018). Statistical Analysis of Reliable and Secure Transmission Gate based Arbiter Physical Unclonable Functions (PUFs).*Journal of Computational Information Systems,* 14(3), 62 - 69.

[38] Puliyath, S. (2014). Advanced Secure Scan Design against Scan Based Differential Cryptanalysis. *International Journal of Advances in Engineering and Emerging Technology, 5*(6), 274-279.

[39] Rinesh, S., and Jagadeesan, S. (2014). Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. *Excel International Journal of Technology, Engineering and Management, 1*(1), 17-20.

[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.