Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2017 12 (3): 152-158

Privacy Preserving Multi Sharing Control for Big Data Storage

Dr.S. Philomina, Dr.M. Sundararajan, M. Susila

Received: 10 November 2016 ▪ Revised: 13 December 2016 ▪ Accepted: 12 January 2017

Abstract: Security is a prime concern for any service that provides big data storage. The data of an individual should remain confidential and should be accessed only by any authenticated person. One of the aspects of security that is considered prior storing data is the anonymity of the service clients. The service that is used for storage should provide practical and fine-grained encrypted data sharing in such a way that only a ciphertext of data is shared among others by the data owner under some specified conditions. The required features are obtained by introduction a new technique for providing big data storage i.e., a privacy preserving ciphertext multi sharing mechanism. In this technique the advantages of proxy re-encryption technique are employed that enables ciphertext to be securely and conditionally shared multiple times and it also ensures that the knowledge of underlying message and the identity information of ciphertext senders and recipients is not leaked. The technique is also vulnerable to the chosen ciphertext attacks.

Keywords: Big Data Storage, Multi Sharing Control, Public Key Encryption (PKE).

INTRODUCTION

To Date many individuals and companies choose to upload their data to clouds since the clouds supports considerable data storage service but also efficient data processing capability. Accordingly, it is unavoidable that trillions of personal and industrial data are flooding the Internet. For example, in some smart grid scenario, a governmental surveillance authority may choose to supervise the electricity consumption of a local living district. A great amount of electricity consumed data of each family located inside the district will be automatically transferred to the authority via Internet period by period. The need of big data storage, therefore, is more desirable than ever. Manuscript received; revised; accepted. Date of publication; date of current version. The work of K. Liang was supported in part by the Privacy-Aware Retrieval and Modelling of Genomic Data under Grant 13283250 and in part by the Academy of Finland, Finland. The work of W. Susilo was supported by the Australian Research Council Discovery Project under Grant ARC DP130101383. The work of J. K. Liu was supported by the National Natural Science Foundation of China under Grant 61472083. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Liqun Chen. *(Corresponding author: Joseph K. Liu.)* K. Liang is with the Department of Computer Science, Aalto University,

Espoo 02150, Finland (e-mail: kaitai.liang@aalto.fi).

W. Susilo is with the Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia (e-

J.K. Liu is with the Faculty of Information Technology, Monash University, Melbourne, VIC 3800, Australia Color versions of one or more of the figures in this paper are available online at A basic security requirement of big data storage is to guarantee the confidentiality of the data. Fortunately, some existing cryptographic encryption mechanisms can be employed to fulfill the requirement. For instance, Public Key Encryption (PKE) allows a data sender to encrypts the data under the public key of receiver such that no one except the valid recipient can gain access to the data. Nevertheless, this does not satisfy all the requirements of users in the scenario of big data storage. Consider the following scenario. We suppose a

Dr.S. Philomina, Assistant Professor, Department of Electronics and Communication Engineering, BIST, BIHER, Bharath Institute of Higher, Education & Research, Selaiyur, Chennai. E-mail: philomina.ece@bharathuniv.ac.in

Dr.M. Sundararajan, Professor, Department of Electronics and Communication Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

M. Susila, Assistant Professor, Department of Electronics and Communication Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

hospital. Stores its patients' medical records in a cloud storage system and meanwhile, the records are all encrypted so as to avoid the cloud server from accessing to any patient's medical information. After a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. By using some traditional PKE, Identity-Based Encryption (IBE), or Attribute-Based Encryption (ABE), the confidentiality of the record can be protected effectively. By trivially employing traditional encryption mechanisms (to guarantee the confidentiality of medical record), nevertheless,

We cannot prevent some sensitive personal information from being leaked to the cloud server but also the public. This is because traditional encryption systems do not consider the anonymity of a ciphertext sender/receiver. Accordingly, someone, could be anyone with capability of obtaining a ciphertext may know whose public key the ciphertext is encrypted under, namely who is the owner of the ciphertext, such that the patient associated with the ciphertext can be easily identified. Similarly, the recipient/destination of the ciphertext, e.g., Cardiology Dept., can be known from the ciphertext without any difficulty as well. This seriously disgraces the privacy of patient.

Moreover, a patient might be transferred to more than one medical department in different treatment phases. The corresponding medical record then needs to be converted to the ciphertexts corresponding to various receivers so as to be shared among the departments. Therefore, the update of ciphertext recipient is desirable. Precisely speaking, a fine-grained ciphertext update for receivers is necessary in the sense that a ciphertext can be conditionally shared with others. The medical record owner, e.g., the patient, has rights to decide who can gain access to the record, and which kinds of data are allowed for access. For example, the patient can choose to specify that only the medical record described with "teeth" can be read by a dentist. This fine-grained control prevents a data sharing mechanism from being limited to the "all-or-nothing" share mode.

Personal use is permitted, but republication/redistribution requires IEEE permission. This research work aims to solve the above problems. To preserve anonymity, some well-known encryption mechanisms are proposed in the literature, such as anonymous IBE [8]. By employing these primitives, the source and the destination of data can be protected privately. However, the primitives cannot support the update of ciphertext receiver. There are some naive approaches to update ciphertext's recipient. For instance, data owner can employ the decrypt then- re-encrypt mode. Nonetheless, this is applicable to the scenario where there is only a small amount of data. If the encrypted data is either a group of sequences of genome information or a network audit log, the decryption and re-encryption might be time consumed and computation costly. Moreover, this mode also suffers from a limitation that the data owner has to be on-line all the time.

Our Contributions

In this paper, we aim to propose a ciphertext sharing mechanism with the following properties:

- Anonymity: given a ciphertext, no one knows the identity information of sender and receiver.
- Multiple receiver-update: given a ciphertext, the receiver of the ciphertext can be updated in multiple times. In this Paper, we refer to this property as "multi-hop".
- Conditional sharing: a ciphertext can be fine-grained shared with others if the pre-specified conditions are satisfied.

Achievements: We investigate a new notion, AMH-IBCPRE.

- The security model of MH-IBCPRE is the basic one, in which a challenger plays the game with the adversary to launch Chosen-Ciphertext Attacks (CCA) to the original ciphertext and re-encrypted ciphertext in order to solve a hard problem.
- We also consider the case where a proxy colludes with delegatee to compromise the underlying message and the secret key of delegator. Here, the protection of themessage is very difficult to achieve as the delegatee can always decrypt the corresponding ciphertext for the proxy. The secret key of the delegator, however, is possible to be secured.
- For the definition of collusion attacks model, we allow an adversary to acquire all re-encryption keys, and the adversary wins the game if it outputs a valid secret key of an uncorrupted user. We note that our definition is in the selective model in which the adversary has to output a target identity at the outset of the game.
- As to the security model of anonymity, it is complicated in the sense that we categorize the game into two subgames: one is the anonymity for delegator (i.e. given the original ciphertext an adversary cannot output the identity of delegator), the other is the anonymity of re-encryption

key (i.e. an adversary cannot distinguish a valid re-encryption key from a random one belonging to re-encryption key space).We next propose a concrete construction for unidirectional.

Related Work

Here, we compare our work with the some related systems, and summarize the comparison of properties in Table I. While multiple ciphertext receiver update (denoting as M.U.), conditional (data) share, collusion resistance (denoting as C.R.), anonymity, and without random oracle (denoting as W.R.O.), have all five been partially achieved by previous schemes, 1We refer to multiple ciphertext receiver update to a notion called Multi-Hop (MH) in this paper. Functionality and SECURITY comparison there is no effective CCA-secure proposal that achieves all properties simultaneously in the standard model. This paper, for the first time, fills the gap.

SYSTEM DEFINITION AND THREAT MODELS

System Definition

Definition 1: A unidirectional Multi-Hop Identity-Based Conditional Proxy Re-Encryption (MH-IBCPRE) scheme consists of the following algorithms:

1. *(mpk, msk)←Setup (1k):* on input a security parameter *k*, output a master public key *mpk* and a master secret key *msk*. For simplicity, we omit *mpk* in the expression of the following algorithms.
2. *skI D ← KeyGen(msk, ID):* on input *msk*, and an identity *I D* ∈ {0, 1}∗, output a secret key *skI D*.
3. *rkw,I Di→I Di_ ← ReKeyGen(I Di , skI Di , I Di⌟ w):* on input a delegator's identity *I Di* and the corresponding secret key *skI Di* , a delegatee's identity *I Di* , and a condition *w* ∈ {0, 1}∗, output a re-encryption key *rkw,I Di→I Di_* from *I Di* to *I Di_* under condition *w*.
4. *C*1*,I Di,w ← Enc(IDi , w, m):* on input an identity *I Di*, a condition *w* and a message *m*, output a 1-level ciphertext *C*1*,I Di,w* under identity *I Di* and *w*.
5. *Cl*+1*,I Di_ ,w ← ReEnc(rkw,I Di→I Di⌟ Cl,I Di ,w):* on input *rkw,I Di→I Di⌟* and an *l*-level ciphertext *Cl,I Di ,w* under identity *I Di* and *w*, output an *(l* + 1*)*-level ciphertext *Cl*+1*,I Di_ ,w* under identity *I Di_* and *w* or ⊥ for failure, where *l* ≥ 1*, l* ∈ N.
6. *m ← Dec(skI Di ,Cl,I Di ,w):* on input *skI Di* , and an *l*-level ciphertext *Cl,I Di ,w* under identity *I Di* and *w*, output a message *m* or ⊥ for failure, where *l* ≥ 1*, l* ∈ N. LIANG *et al.*: PRIVACY-PRESERVING CIPHERTEXT MULTI-SHARING CONTROL FOR BIG DATA STORAGE 1581

Threat Models

We define four models in terms of the selective condition and selective identity chosen ciphertext security (IND-sConsID- CCA), collusion resistance, the anonymity of the original ciphertext and anonymity of the re-encryption key in this section. Before proceeding, we define some notations.

- *Delegation Chain:* There is a set of re-encryption

keys *RK* = {*rkw, I Di*1 *→I Di*2 *, . . . , rkw, I Dil*−1 *→I Di* } under the same condition *w*, for any re encryption key *rkw, I Di j →I Di j*+1 in *RK*, *I Di j* = *I Di j*+1 . We say that there exists a delegation chain under *w* from identity *I Di*1 to identity *I Dil*, denoted as *w*|*I Di*1→ *. . .* → *I Dil*. Note this delegation chain includes the case where *I Di*1 = *I Dil*. Besides, we use *w*|*I D* to indicate a ciphertext under *w* and *I D*, and for a single identity *I D* we use ⊥ |*I D* to denote it.

- *Uncorrupted/Corrupted Identity:* If the secret key of an identity is compromised by an adversary, the identity is a corrupted identity. Else, it is an uncorrupted identity.
- *Uncorrupted Delegation Chain:* Suppose there is a delegation chain under *w* from *I Di* to *I Dj.*

(i.e. *w*|*I Di* → *...* → *I Dj*). If there is no corrupted identity in the chain, it is an uncorrupted delegation chain., it is corrupted.

Definition 2: A unidirectional MH-IBCPRE scheme is IND-sCon-sID-CCA-secure if no PPT adversary *A* can win the game below with non-negligible advantage. In the game, *B* is the game challenger and *k* is the security parameter.

1. **Init.** *A* outputs a challenge identity *I D*∗ ∈ {0, 1}∗ and a challenge condition *w* ∈ {0, 1}∗.
2. **Setup.** *B* runs *setup (*1*k)* and returns *mpk* to *A*.
3. **Phase 1.** *A* is given access to the following oracles. a) *Osk (ID):* given an identity *I D*, output *skI D* ← *KeyGen(msk, I D)*.
   1. *Ork (IDi , I Di⌟w):* on input two distinct identities *I Di* and *I Di⌟* and a condition *w*, output *rkw, I Di→I Di_* ← *ReKeyGen(I Di* , *skI Di* , *I Di_* , *w)*, where *skI Di* ← *KeyGen(msk*, *I Di)*.

2. *Ore(IDi , I Di_, w, Cl, I Di ,w):* on input two distinct identities *I Di* and *I Di_* , a condition *w*, and an *l*-level ciphertext *Cl, I Di ,w* under *I Di* and *w*, output *Cl*+1*,I Di ,w* ← *ReEnc(rkw,I Di*→*I Di_ , Cl,I Di ,w)*, where *rkw,I Di*→*I Di_* ← *ReKeyGen(I Di , skI Di , I Di_ , w)*, *skI Di* ← *KeyGen(msk, I Di)*.
3. *Odec(IDi ,Cl,I Di ,w):* on input an identity *I Di*, and an *l*-level ciphertext *Cl, I Di ,w*, output *m* ← *Dec(skI Di ,Cl,I Di ,w)*, where *skI Di*←*KeyGen(msk, I Di)*. In this phase the followings are forbidden to issue:

- *Osk (I D)* for any *I D*, if there is an uncorrupted delegation chain under *w*∗ from *I D*∗ to *I D*, or *I D*∗ = *I D*.
- *Ork (I Di , I Di_,w*∗*)* for any *I Di, I Di_*, if there is an uncorrupted delegation chain under *w*∗ from *I D*∗ to *I Di* or *I D*∗ = *I Di*, but *I Di_* is in a corrupted delegation chain.

4. Challenge**.** *A* outputs two equal length messages *m*0, *m*1, and a set of identities {*I Di j* } *j*=*l*∗−1 *j*=1 to *B*. *B* computes *Cl*∗*,I D*∗*,w*∗ as *ReEnc(ReKeyGen(I Dil*∗−1 *, skI Dil*∗−1 *, I D*∗ *,w*∗ *ReEnc(ReKeyGen(I Dil*∗−2 *, skI Dil*∗−2*, I Dil*∗−1*,w* ∗ *), ... , ReEnc(ReKeyGen(I Di*1 *, skI Di*1*, I Di*2*,w* ∗ *), Enc(I Di*1*,w* ∗*,mb)))),* where *l*∗ ≥ 2*, l*∗ ∈ N*, b* ∈*R* {0, 1}. Note that we here put *I D*∗ to the *l*∗ level of the ciphertext. This shows no difference from putting it in the first level of the ciphertext since the system supports multi-hop property.
5. **Phase 2.** Same as in **Phase 1** except the followings:

   a) *Ore(IDi , I Di_,w*∗*,Cl,I Di ,w*∗ *):* if *(I Di ,Cl,I Di ,w*∗ *)* is a derivative of *(I D*∗*,Cl*∗*,I D*∗*,w*∗*)*, and *I Di_* is in a corrupted delegation chain. As of [11], a derivative of *(I D*∗*, Cl*∗*, I D*∗*, w*∗*)* is defined.

6. **Guess.** *A* outputs a guess *b_* ∈ {0, 1}. If *b_* = *b*, *A* wins. The advantage of *A* is defined as _ = *AdvI ND-sCon-s ID-CCA MH-I BCPRE, A (*1*k)* = |*Pr*[*b_* = *b*] − 12 |. We now proceed to collusion resistance that guarantees that an adversary cannot compromise the entire secret key of a delegator even if it colludes with the delegatee. *Definition 3:* A unidirectional MH-IBCPRE scheme holds against selective collusion attacks if the advantage *AdvCR A (*1*k)* is negligible for any PPT adversary *A* in the following experiment. Set *O*1 = {*Osk*, *Ork* } and *AdvCR A (*1*k)* as*Pr*[*skI D*∗ ∈ _: *(I D*∗*, State)* ← *A(*1*k)*; *(mpk, msk)*← *Setup(*1*k)*; *skI D*∗ ←*AO*1 *(mpk, State)*] where *k* is the security parameter, *State* is the state information, *I D*∗ is the target and uncorrupted identity, *Osk* and *Ork* are the oracles defined in below with non-negligible advantage.

   1. Init**.** *A* outputs a delegator's identity *I D_*, a challenge delegatee's identity *I D*∗, and a challenge condition *w*∗.
   2. Setup**.** Same as Definition 2.
   3. Phase 1. *A* is allowed to issue queries to *Osk,Ork* , *Ore* and *Odec* which are the oracles defined Definition 2 with the same restrictions.
   4. Challenge. If the following queries

   - *Osk(I Di)* for any *I Di* , if there is an uncorrupted delegation chain under *w*∗ from *I D*∗ to *I Di*, or *I D*∗ = *I Di.*
   - *Ork (I Di , I Dj,w*∗*)* for any *I Di* , *I Dj*, if there is an uncorrupted delegation chain under *w*∗ from *I D*∗ to *I Di* or *I D*∗ = *I Di*, but *I Dj* is in a corrupted delegation chain. Are never made, *B* flips a coin-toss for *b* ∈ {0, 1}.

   5. Phase 2. Same as Phase 1 except the followings:

   a) *Osk(I Di)* for any *I Di* , if there is an uncorrupted delegation chain under *w*∗ from *I D*∗ to *I Di*, or *I D*∗ = *I Di* ;

   b) *Ork (I Di , I Dj,w*∗*)* for any *I Di* , *I Dj*, if there is an uncorrupted delegation chain under *w*∗ from *I D*∗ to *I Di* or *I D*∗ = *I Di*, but *I Dj* is in a corrupted delegation chain;

   c) *Ore(IDi , I Di_,w*∗*,Cl,I Di ,w*∗ *):* if *(I Di ,Cl,I Di ,w*∗ *)* is a (derivative of) ciphertext generated by a re-encryption key in the delegation chain under *w*∗ from *I D*∗ to *I Di* , and *I Di_* is in a corrupted delegation chain.

PRELIMINARIES

Asymmetric Pairing

Let *BSetup* be an algorithm that on input the security parameter *k*, outputs the parameters of a bilinear map as *(q, g, ˆg,*G1,G2,G*T , e)*, where G1, G2 and G*T* are multiplicative cyclic groups of prime order *q*, where |*q*| = *k*, and *g* is a random generator of G1, ˆ*g* is a random generator of G2. The mapping *e* : G1 ×G2 → G*T* has three properties:

1. *Bilinearity*: for all *a, b* ∈*R* Z ∗*q* , *e(ga,* ˆ *gb)* = *e(g,* ˆ*g)ab*;

2. *Non-degeneracy*: $e(g, \hat{}g) = 1\mathrm{G}T$, where $1\mathrm{G}T$ is the unit of $\mathrm{G}T$; (3) *Computability*: e can be efficiently computed. *Asymmetric Decisional BDH (ADBDH) Problem [14]:* Given a tuple $(g, ga, gc, \hat{}\ g, \hat{}\ ga, \hat{}\ gb) \in \mathrm{G}31 \times \mathrm{G}32$ and $T \in \mathrm{G}T$, decide whether $T = e(g, \hat{}\ g)abc$. *(Asymmetric) Decisional P-BDH Problem [14]:* Given a tuple $(g, ga, gab, gc, \hat{}\ g, \hat{}\ ga, \hat{}\ gb) \in \mathrm{G}41 \times \mathrm{G}32$ and $T \in \mathrm{G}T$, decide whether $T = e(g, \hat{}g)abc$.

An Anonymous IBE and Its Extensions

Ducas [14] introduces an efficient anonymous IBE (Du-ANO-IBE) scheme in the standard model. We review its construction below, and omit the definition and security model of Du-ANO-IBE as the details can be found in [14].

- *Setup (1k):* run $(q, g, \hat{}g, \mathrm{G}1, \mathrm{G}2, \mathrm{G}T , e) \leftarrow BSetup(1k)$, choose random values $\alpha, \beta, \gamma, \delta, \eta \in \mathrm{Z} *q$ and set $g1 = g\alpha$, $g2 = g\beta$, $h = g\gamma$, $f = g\delta$, $t = g\eta$, $g\hat{}1 = g\hat{}\alpha$, $\hat{}\ g2 = \hat{}\ g\beta$, $\hat{}h = g\hat{}\gamma$, $f\hat{} = g\hat{}\delta$, $t\hat{} = g\hat{}\eta$. The master secret key $msk = (g\hat{}0 = g\hat{}\alpha\beta, f\hat{}, t\hat{})$, the master public key $mpk = (g, \hat{}\ g, g1, h, f, t, \hat{}\ g2, \hat{}h)$.
- *Extract(msk, ID):* given msk and an identity $I\,D \in \mathrm{Z} *q$, randomly choose $r, R \in \mathrm{Z} *q$, output $skI\,D = (skI\,D0 , skI\,D1 , skI\,D2\ ) = (\hat{}\ g0(\hat{}h\ I\,D\,f\hat{})r\,t\hat{}R, g\hat{}r , g\hat{}\ R)$.
- *Enc(mpk, ID, m):* randomly choose $s \in\ *q$, compute $C1 = e(g1, \hat{}\ g2)s \cdot m$, $C2 = gs$, $C3 = (hI\,D\,f\,)s$, $C4 = ts$, and output the ciphertext $C = (C1,C2,C3,C4)$, where $I\,D \in \mathrm{Z} *q$, $m \in \mathrm{G}T$.
- *Dec(skI D, C):* given a ciphertext $C = (C1,C2,C3,C4)$, using the private key $skI\ D$ to recover the plaintext $m = C1 \cdot e(C3, skI\,D1\ ) \cdot e(C4, skI\,D2\ )/e(C2, skI\,D0\ )$.

SYSTEM CONSTRUCTION

Construction Details

We allow condition and identities to be arbitrary length, but they should be hashed by a Target Collision Resistant (TCR) hash function [13] $H0$: $\{0, 1\}* \rightarrow \mathrm{Z} *q$ beforehand.

- *Setup(1k):* Given k, run $(q, g, \hat{}g, \mathrm{G}1, \mathrm{G}2, \mathrm{G}T , e) \leftarrow BSetup(1k)$. Let $w \in \mathrm{Z} *q$ be a condition. Choose $\alpha, \beta, \gamma , \delta1, \delta2, \delta3, \eta \in R\ \mathrm{Z} *q$, and set $g1 = g\alpha$, $g2 = g\beta$, $h = g\gamma$, $f1 = g\delta1$, $f2 = g\delta2$, $f3 = g\delta3$, $t = g\eta$, $\hat{}\ g1 = \hat{}g\alpha$, $\hat{}\ g2 = \hat{}g\beta$, $\hat{}h = g\hat{}\gamma$, $f\hat{}1 = g\hat{}\delta1$, $f\hat{}2 = g\hat{}\delta2$, $f\hat{}3 = g\hat{}\delta3$, $t\hat{} = g\hat{}\eta$.

CONCLUSIONS

We introduced a novel notion, anonymous multi-hop identity-based conditional proxy re-encryption, to preserve the anonymity for ciphertext sender/receiver, conditional data sharing and multiple recipient-update. We further proposed a concrete system for the notion. Meanwhile, we proved the system CCA-secure in the standard model under the decisional P-bilinear Diffie-Hellman assumption. To the best of our knowledge, our primitive is the first of its kind in the literature.

REFERENCES

[1] Krishnamoorthy, P., & Jayalakshmi, T. (2012). Preparation, characterization and synthesis of silver nanoparticles by using phyllanthusniruri for the antimicrobial activity and cytotoxic effects, *Journal of Chemical and Pharmaceutical Research, 4*(11), 4783-4794.

[2] Amir, M., Gungunes, H., Slimani, Y., Tashkandi, N., El Sayed, H.S., Aldakheel, F., Sertkol, M., Sozeri H., Manikandan A., Ercan, I., & Baykal, A. (2019). Mössbauer studies and magnetic properties of cubic CuFe 2 O 4 nanoparticles. *Journal of Superconductivity and Novel Magnetism*, *32*(3), 557-564.

[3] Raj, M.S., Saravanan T., & Srinivasan, V. (2014). A modified direct torque control of induction motor using space vector modulation technique. *Middle - East Journal of Scientific Research, 20*(11), 1572-1574.

[4] Khanaa, V., & Thooyamani, K.P. (2013). Using triangular shaped stepped impedance resonators design of compact microstrip quad-band. *Middle-East Journal of Scientific Research*, *18*(12), 1842-1844.

[5] Asiri S., Sertkol M., Güngüneş H., Amir M., Manikandan A., Ercan I., & Baykal A. (2018). The Temperature Effect on Magnetic Properties of NiFe 2 O 4 Nanoparticles. *Journal of Inorganic and Organometallic Polymers and Materials, 28*(4), 1587-1597.

[6] Thaya, R., Malaikozhundan, B., Vijayakumar, S., Sivakamavalli, J., Jeyasekar, R., Shanthi, S., Vaseeharan, B., Ramasamy, P., & Sonawane, A. (2016). Chitosan coated Ag/ZnO nanocomposite and their antibiofilm, antifungal and cytotoxic effects on murine macrophages. *Microbial pathogenesis*, *100*, 124-132.

[7] Kolanthai, E., Ganesan, K., Epple, M., & Kalkura, S.N. (2016). Synthesis of nanosized hydroxyapatite/agarose powders for bone filler and drug delivery application. *Materials Today Communications*, *8*, 31-40.

[8] Thilagavathi, P., Manikandan, A., Sujatha, S., Jaganathan, S.K., & Arul Antony, S. (2016). Sol–Gel Synthesis and Characterization Studies of NiMoO4 Nanostructures for Photocatalytic Degradation of Methylene Blue Dye. *Nanoscience and Nanotechnology Letters*, *8*(5), 438-443.

[9] Thamotharan C., Prabhakar S., Vanangamudi, S., & Anbazhagan, R. (2014). Anti-lock braking system in two wheelers. *Middle - East Journal of Scientific Research, 20*(12), 2274-2278.

[10] Thamotharan C., Prabhakar S., Vanangamudi, S., Anbazhagan, R., & Coomarasamy C. (2014). Hydraulic rear drum brake system in two wheeler. *Middle - East Journal of Scientific Research, 20*(12), 1826-1833.

[11] Vanangamudi, S., Prabhakar S., Thamotharan C., & Anbazhagan, R. (2014). Collision control system in cars. *Middle - East Journal of Scientific Research, 20*(12), 1799-1809.

[12] Vanangamudi S., Prabhakar S., Thamotharan C., & Anbazhagan R. (2014). Drive shaft mechanism in motor cycle. *Middle - East Journal of Scientific Research, 20*(12), 1810-1815.

[13] Anbazhagan R., Prabhakar S., Vanangamudi S., & Thamotharan C. (2014). Electromagnetic engine. *Middle - East Journal of Scientific Research, 20*(3), 385-387, 2014.

[14] Kalaiselvi, V.S., Prabhu, K., & Mani Ramesh, V.V. (2013). The association of serum osteocalcin with the bone mineral density in post-menopausal women. *Journal of clinical and diagnostic research: JCDR*, *7*(5), 814-816.

[15] Kalaiselvi, V.S., Saikumar, P., & Prabhu, K. (2012). The anti mullerian hormone-a novel marker for assessing the ovarian reserve in women with regular menstrual cycles. *Journal of clinical and diagnostic research: JCDR*, *6*(10), 1636-1639.

[16] Arul, K.T, Manikandan, E., Ladchumananandasivam, R., & Maaza, M. (2016). Novel polyvinyl alcohol polymer based nanostructure with ferrites co-doped with nickel and cobalt ions for magneto-sensor application. *Polymer International*, *65*(12), 1482-1485.

[17] Das, M.P., & Kumar, S. (2015). An approach to low-density polyethylene biodegradation by Bacillus amyloliquefaciens. *3 Biotech*, *5*(1), 81-86.

[18] Vanangamudi S., Prabhakar S., Thamotharan C., & Anbazhagan, R. (2014). Turbo charger in two wheeler engine. *Middle - East Journal of Scientific Research, 20*(12), 1841-1847.

[19] Vanangamudi S., Prabhakar S., Thamotharan C., & Anbazhagan, R. (2014). Design and calculation with fabrication of an aero hydraulwicclutch. *Middle - East Journal of Scientific Research, 20*(12), 1796-1798, 2014.

[20] Saravanan, T., Raj, M.S., & Gopalakrishnan, K. (2014). VLSI based 1-D ICT processor for image coding. *Middle-East Journal of Scientific Research*, *20*(11), 1511-1516.

[21] Ajona, M., & Kaviya, B. (2014). An environmental friendly self-healing microbial concrete. *International Journal of Applied Engineering Research*, *9*(22), 5457-5462.

[22] Hemalatha, R., & Anbuselvi, S. (2013). Physicochemical constituents of pineapple pulp and waste. *Journal of Chemical and Pharmaceutical Research*, *5*(2), 240-242.

[23] Langeswaran, K., Revathy, R., Kumar, S.G., Vijayaprakash, S., & Balasubramanian, M.P. (2012). Kaempferol ameliorates aflatoxin B1 (AFB1) induced hepatocellular carcinoma through modifying metabolizing enzymes, membrane bound ATPases and mitochondrial TCA cycle enzymes. *Asian Pacific Journal of Tropical Biomedicine*, *2*(3), S1653-S1659.

[24] Masthan, K.M.K., Babu, N.A., Dash, K.C., & Elumalai, M. (2012). Advanced diagnostic aids in oral cancer. *Asian Pacific Journal of Cancer Prevention*, *13*(8), 3573-3576.

[25] Asiri S., Güner S., Demir A., Yildiz A., Manikandan A., & Baykal, A. (2018). Synthesis and Magnetic Characterization of Cu Substituted Barium Hexaferrites. *Journal of Inorganic and Organometallic Polymers and Materials,* 28(3), 1065-1071.

[26] Vellayappan, M.V., Jaganathan, S.K., & Manikandan, A. (2016). Nanomaterials as a game changer in the management and treatment of diabetic foot ulcers. *RSC Advances*, *6*(115), 114859-114878.

[27] Vellayappan, M.V., Venugopal, J.R., Ramakrishna, S., Ray, S., Ismail, A.F., Mandal, M., Manikandan, A., Seal, S., & Jaganathan, S.K. (2016). Electrospinning applications from diagnosis to treatment of diabetes. *RSC Advances*, *6*(87), 83638-83655.

[28] Bavitra, K., Sinthuja, S., Manoharan, N., & Rajesh, S. (2015). The high efficiency renewable PV inverter topology. *Indian Journal of Science and Technology*, *8*(14), 1.

[29] Vanangamudi, S., Prabhakar, S., Thamotharan, C., & Anbazhagan, R. (2014). Design and fabrication of dual clutch. *Middle-East Journal of Scientific Research*, *20*(12), 1816-1818.

[30] Sandhiya, K., & Kaviya, B. Safe bus stop location in Trichy city by using gis. *International Journal of Applied Engineering Research*, *9*(22), 5686-5691.

[31] Selva Kumar, S., Ram Krishna Rao, M., Deepak Kumar, R., Panwar, S., & Prasad, C.S. (2013). Biocontrol by plant growth promoting rhizobacteria against black scurf and stem canker disease of potato caused by Rhizoctonia solani. *Archives of Phytopathology and Plant Protection*, *46*(4), 487-502.

[32] Sharmila, S., & Jeyanthi Rebecca, L. (2012). GC-MS Analysis of esters of fatty acid present in biodiesel produced from Cladophora vagabunda. *Journal of Chemical and Pharmaceutical Research*, *4*(11), 4883-4887.

[33] Ramkumar, M., Rajasankar, S., Gobi, V.V., Dhanalakshmi, C., Manivasagam, T., Thenmozhi, A.J., Essa, M.M., Kalandar, A., & Chidambaram, R. (2017). Neuro protective effect of Demethoxycurcumin, a natural derivative of Curcumin on rotenone induced neurotoxicity in SH-SY 5Y Neuroblastoma cells. *BMC complementary and alternative medicine*, *17*(1), 217.

[34] Selvi, S.A., & Sundararajan, M. (2016). A Combined Framework for Routing and Channel Allocation for Dynamic Spectrum Sharing using Cognitive Radio. *International Journal of Applied Engineering Research*, *11*(7), 4951-4953.

[35] Krupaa R.J., Sankari S.L., Masthan K.M.K., & Rajesh E. (2015). Oral lichen planus: An overview. *Journal of Pharmacy and Bioallied Sciences, 7,* S158-S161.

[36] Srividya, T., & Saritha, B. (2014). Strengthening on RC beam elements with GFRP under flexure. *International Journal of Applied Engineering Research*, *9*(22), 5443-5446.

[37] Kumar, J., Sathish Kumar, K., & Dayakar, P. (2014). Effect of microsilica on high strength concrete. *International Journal of Applied Engineering Research*, *9*(22), 5427-5432.

[38] Saraswathy, R., & Saritha, B. (2014). Planning of integrated satellite township at Thirumazhisai. *International Journal of Applied Engineering Research*, *9*(22), 5558-5560.

[39] Saritha, B., Ilayaraja, K., & Eqyaabal, Z. (2014). Geo textiles and geo synthetics for soil reinforcement. *International Journal of Applied Engineering Research*, *9*(22), 5533-5536.

[40] Iyappan, L., & Dayakar, P. (2014). Identification of landslide prone zone for coonoor taluk using spatial technology. *International Journal of Applied Engineering Research*, *9*(22), 5724-5732.

[41] Aravind, D., & Deepa, K. (2015). Power Improvement of Photovoltaic System Using IEDM in Smart Grid Application. *Excel International Journal of Technology, Engineering and Management, 2*(2), 22-26.

[42] Naveen, N., & Rajesh Kumar, B. (2015). Automatic LPG Drum Level Pointer and SMS Booking System with Refuge. *Excel International Journal of Technology, Engineering and Management, 2*(2), 27-29.

[43] Dr.Veenadhari, S. (2016). Crop Advisor: A Software Tool for Forecasting Paddy Yield. *Bonfring International Journal of Data Mining, 6*(3), 34-38.

[44] Kondori, M.A.P., & Peashdad, M.H. (2015). Analysis of challenges and solutions in cloud computing security. *International Academic Journal of Innovative Research, 2*(8), 1-11.

[45] Kargar, M.J., & Motaghian, S. (2015). Creating Semi – Automatic Ontology on Persian Wikipedia Texts. *International Academic Journal of Innovative Research, 2*(8), 38-44.

[46] Sandhiya, K., & Yamuna, L. (2014). High Performance Dual-Band Printed Doublet Design Loaded with Split Resonator Structures. *International Journal of Communication and Computer Technologies, 2*(1), 64-67.

[47] Lenin, G.J.N., Noora, J.A., Packiyalakshmi, D., Priyatharshini, S., & Thanapriya, T. (2014). Highly Directive Rectangular Patch Antenna Arrays. *International Journal of Communication and Computer Technologies, 2*(1), 68-73.

[48] Oh, T.J., & Anthony, (2017). New and Fast Emerging Advance Structure of Text Mining from Unstructured Data. *Bonfring International Journal of Industrial Engineering and Management Science, 7*(2), 13-16.

[49] Janmohammadi, P., & Babazade, M. (2015). Resource Management in the Cloud Computing Using a Method Based on Ant Colony Optimization. *International Academic Journal of Science and Engineering, 2(*6), 40-54.

[50] Farajizadeh, M., & Bakhsh, N.N. (2015). A mechanism to improve the throughput of cloud computing environments using congestion control. *International Academic Journal of Science and Engineering, 2*(7), 10-24.