Novel Approach for Control Data Theft Attack in Cloud Computing

K. Narasimha Sastry, B. Thirumala Rao, T. Gunasekhar
Dept of CSE, K L University, India

Article Info

Article history:

Received May 27, 2015
Revised Aug 12, 2015
Accepted Sep 2, 2015

Keyword:

Insider
Jeopardize
Mitigate
Preeminent

ABSTRACT

Information security is a major problem faced by cloud computing around the world. Because of their adverse effects on organizational information systems, viruses, hackers, and attackers insiders can jeopardize organizations capabilities to pursue their undertaken effectively. Although technology based solutions help to mitigate some of the many problems of information security, even the preeminent technology can't work successfully unless effective human computer communication occurs.IT experts, users and administrators all play crucial role to determine the behavior that occurs as people interact with information technology will support the maintenance of effective security or threaten it. In the present paper we try to apply behavioral science concepts and techniques to understanding problems of information security in organizations.

Corresponding Author:

K. Narasimha Sastry,
Dept of CSE,
K L University.
Email: sastrysays@gmail.com

1. INTRODUCTION

Cloud storage is a model of networked enterprise Cache where data is stored in virtualized pools of storage. Storing, Outsourcing datain Cloud has become an extremely convenient choice for the business sector. In spite of an excellent operational efficiency, storing data on cloud has its own set of drawbacks which impossible to avoid. Stealing the user credentials by Masqueraders mimic legitimate users when they access of Cloud. When the masqueraders logs in with the stolen credentials, He or she gets same rights to access the data like real user. These types of attacksare done by insider [2].

The information theft attacks carried out by an insider is one of the top threats to Cloud security. One of the current examples being the credit card data breach at Marriot, Sheraton and other hotels. The company said information of customer's names and numbers on consumers' credit or debit cards, security codes and card expiration dates are theft by cyber criminals. Another example is the one which happened in Berlin. Cell phone, broadband provider Vodafone Deutschland says it was the target of a large scale data theft affecting the personal details of 2 million German customers. Spokesman Alexander Leinhos says the attack was conducted by an unidentified IT systems administrator who worked for a company.

Vodafone said in a statement Thursday that the stolen data included customers' names, addresses, etc. and was done by an insider attacker.Various security mechanisms have focused on ways of preventing illegal and unauthorized access to data present on the Cloud. This has been done through various encryption techniques. Ning Cao, Cong Wang and others proposed an encryption technique based on Multi-keyword Ranked Search which cannot protect against insider attacker. Building the trustworthy cloud is not enough, avoiding data theft attacks is more important. Once the data is lost we could not get it back. Then an idea is proposed which can secure data to some extent i.e. disinformation attack. One example is data theft attack from the Cloud. Several Twitter personal and business documents were ex-filtrated to technological website TechCrunch [2], and customers‟ accounts, Cloud service customer and within personal online social networking profiles by individual users. Cloud storage is amodel of networked enterprise storage where large data is stored [3].

2. SYSTEM MODEL

There are three different entities as in Figure 1. Cloud server, Cloud service provider (CSP) and clients are the data owners. Clients always requests space on the cloud while in registration. The service provider takes the request, processesrequest and access to the client on cloud. The client receive a system created password via email by cloud server. Once the registration is successfully completed the user can access his data and capable to perform upload, download and etc.

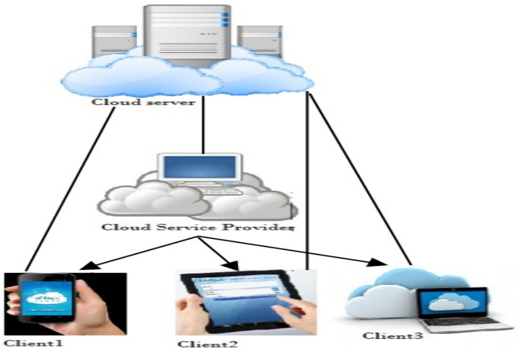


Figure 1. System model

3. SECURING CLOUD WITH FOG

Cloud computing is a technique which provide services to client over the network; user can use any type of services (SaaS, PaaS, IaaS). Cloud storage is the model of network enterprise storage where huge amount of data are stored. Cloud computing provide storage space services for the users, user can stored his data and information in the cloud and he can access to information as store it form any computer connected to the internet [2], [3].the main thing is that the user don't know where and how data is stored ?and who can see the data ? The problem of user when he store sensitive information in the cloud the user require security of thecloud computing to assurance nobody can right to use and view his data and business related information that his store in cloud, to avoid this problem used encryption method. But encryption method unsuccessful in preventing data theft attacks. By applying encryption technique to the information we can't realize total protection to confidential data. In Existing system as per the Literature survey done it is observe that decoy file creation is done whenever new file is being upload to the cloud was suggested but in such case require huge amount of storage space in the cloud [4]. A. Disadvantage 1.It's not identify when the attack is happening. 2. Itsvery complex to identify which user is attack.3. We can't detect the file which was hacking.

4. PROPOSED WORK

In our work we propose a different approach for securing data in the cloud using offensive decoy technology. The data theft by insider is simply passed with the help of creation of decoy file on demand. We check data access in the cloud and identify abnormal data access patterns. When illegal access is supposed and then verified using challenge questions, we launch disinformation attack by returning large amounts of decoy information to the attacker. In the system we develop whenever insider observed to be performing data theft, only then decoy file is created and is passed on to the requesting insider, whenever user trying to upload a file on the cloud user provide security question. The same security question appear when any user want to download or do any operation perform on the particular file form the cloud. Incase insider tries to download the same file once again the usage of time stamp based key gives him a new decoy file as compared to the previous which will confuse him. This protects against the misuse of the user's real data.

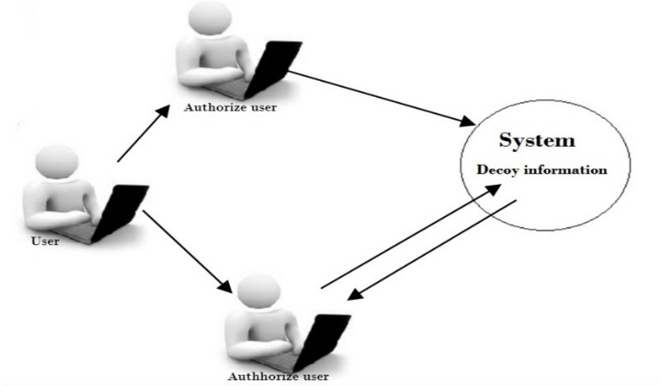


Figure 2. Block Diagram of Proposed system

We are providing an OTP system at the user level in this system. The OTP system will generate a verification code which the user required to enter during registration. After this code will be confirmed by the TPA and only after his authorization the user registration will be done. Next moves to the uploading and downloading of files. While uploading the innovative data will be sent to the CSP and a copy of it would be sent to the TPA for authentication. After a simple yes/no message from the TPA the innovative file will be processed further for division and encryption by the CSP. This will also reduce the overhead significantly. The rights to modify update or delete will only exist in with the owner of the data thereby ensuring a most select level of Security. Internally the DB admin is also monitored by the TPA in order to keep a check on any form of wicked activity. Data lost can also effectively retrieved using standby servers (RAID LEVEL 1). Other specifications in the application include digital signatures.

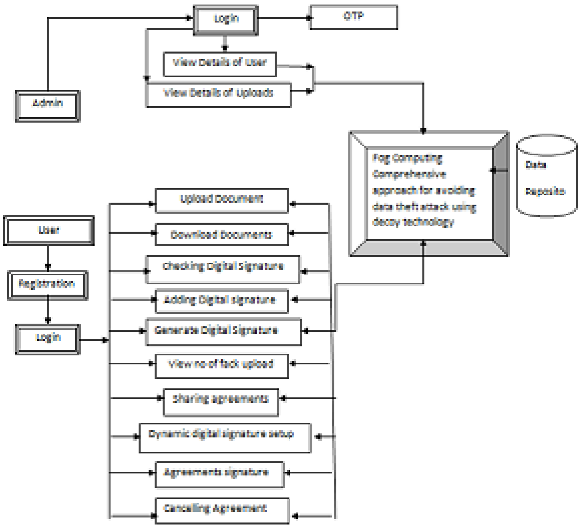


Figure 3. System architecture

5. SECURING CLOUDS

The necessary idea is that we can boundary the injure of stolen information if we decrease the value of that stolen information to the attacker. We can achieve this through a "preventive‟ disinformation attack. We imagine that secure Cloud services can be implemented given two other security features:

1) Confusing the attacker with dummy data we imagine that the combination of these two security features will provide unmatched levels of security in Cloud. Currently the Cloud security method is available that provides this level of security. We have useful these concepts to notice illegal data access to data stored on a local file system by masqueraders, i.e. attackers who copy valid users after theft their identification. Unauthorized access to Cloud data by a rascal insider as the malicious act of a masquerader. Our sample

results in a local file system setting show that combining both procedures can yield better recognition results. The results are recommend that this approach may work in a Cloud environment. The Cloud is proposed to be as clear to the user as a local file system. In the following we analysis briefly some of the trial results achieved by using this approach to detect masquerade activity in a local file setting [9], [11].

2) Description of Research

a) User Behavior Profiling
b) Decoy documents
c) Secure from dealer
d) Block the nasty user
e) Differentiate user

5.1. User Profiling Behavior Module

In this component, admin will going to record log record of all users so that he can easily set working baseline for legal user. Admin monitor data access in the cloud and notice abnormal data access patterns User profiling will a well-known Technique that can be applied here to check how, when, and how much a client access their data in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's data is experience. This method of behavior based security will regularly use in scheme uncovering applications. Such profiles would obviously include volumetric information, how many documents are typically read and how often. We check for abnormal search behaviors that display deviations from the user baseline the connection of search actions difference identification with trap-based decoy files should provide stronger confirmation of malfeasance, and therefore recover a detector's exactness [13].

5.2. Decoy Documents Module

We suggest a different approach for securing data in the cloud using nasty decoy technology. We monitor data access in the cloud and sense irregular data access patterns. We initiate a disinformation attack by recurring large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. We use this technology to begin disinformation attacks against malicious insiders, preventing them from distinguishing the valid aware customer data from bogus useless [9], [11].

5.3. Secure from Dealer

If legal user does not want to give access to the dealer so we can protect that access form dealer. In previous system, dealer can directly access the own or corporate data which is stored on to the cloud. There is no any situation for security of information which is stored on to the cloud. So in our planned system, all the data which is stored on the cloud is confined, it is totally depend on the user to assign access agreement to its data. In case, if dealer want to access the information which is stored on the cloud, it has to gain the private key of that particular user to decrypt the information and this method is get finished via safe key replace algorithm [14], [15].

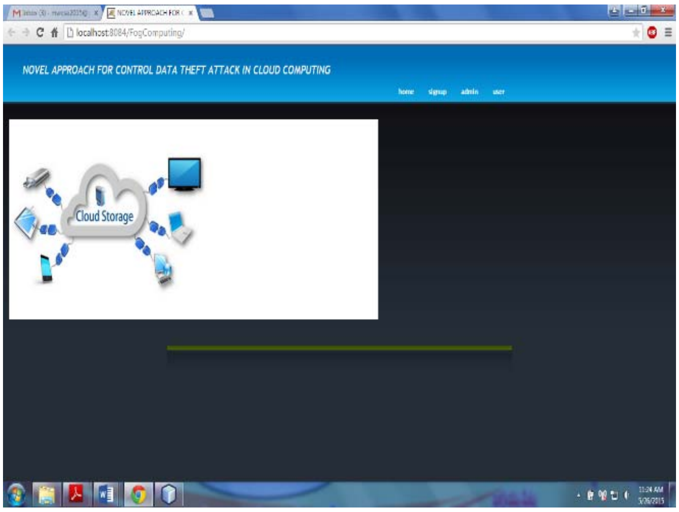
5.4. Block the Nasty User

If we will found any nasty user from his user profile behavior we can directly block that user or we can ask a security questions. For ex. User successively fails in login, animal search attack, uploads files which contains .exe files with in it etc, [13]-[15]. So, all this record of the all user will maintained in the user profiling activities, so as soon as system detects any nasty activities, it directly block that user in case, if any allowed user try to search any other widely stored files then according to our situation our system blocks that client, but during blocking system asks security questions to that user to avoid accepted user jamming [16].

5.5. Differentiate User

We can differentiate user by using contact rights. We can allot human rights at the time of uploading. For example low user have only read permissions, high user has all permissions like modification. By categorizing different users on the cloud, we obtain fair and flexible control on managing resources on the cloud [11].

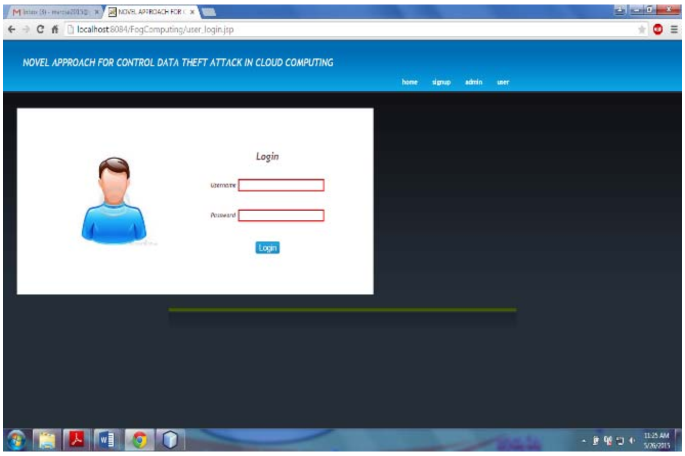
6. IMPLEMENTATION RESULTS



localhost:8084/FogComputing/

NOVEL APPROACH FOR CONTROL DATA THEFT ATTACK IN CLOUD COMPUTING

Figure 4. Home Screen



localhost:8084/FogComputing/user_login.jsp

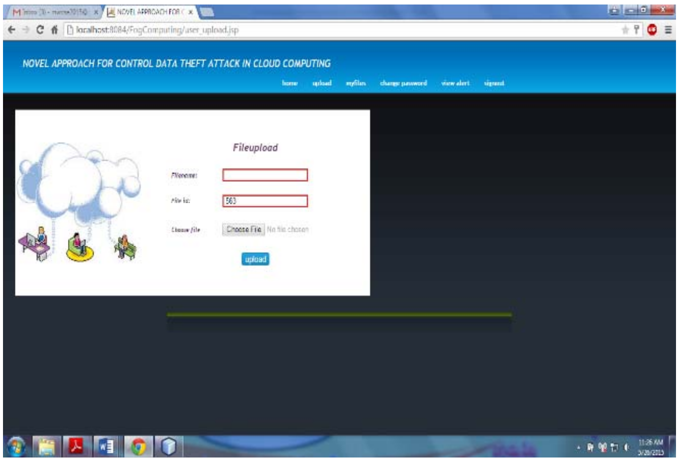
NOVEL APPROACH FOR CONTROL DATA THEFT ATTACK IN CLOUD COMPUTING

Login

Username

Password

Figure 5. User Login



localhost:8084/FogComputing/user_upload.jsp

NOVEL APPROACH FOR CONTROL DATA THEFT ATTACK IN CLOUD COMPUTING

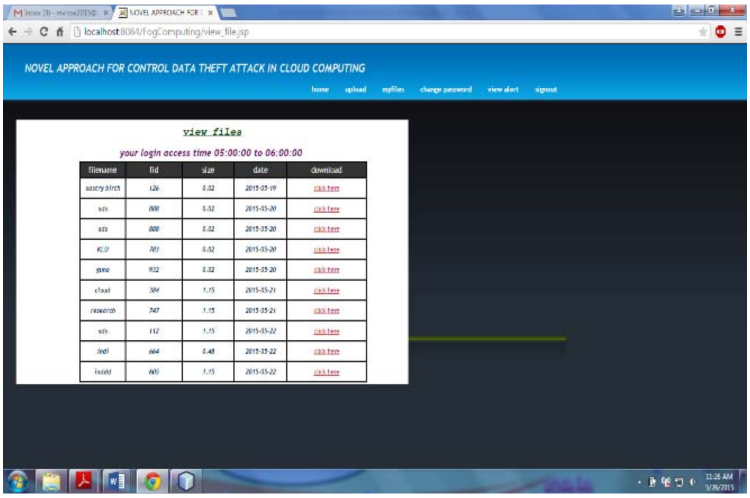
Fileupload

Filename:

File id: 563

Choose file Choose File No file chosen

Figure 6. File Upload to cloud



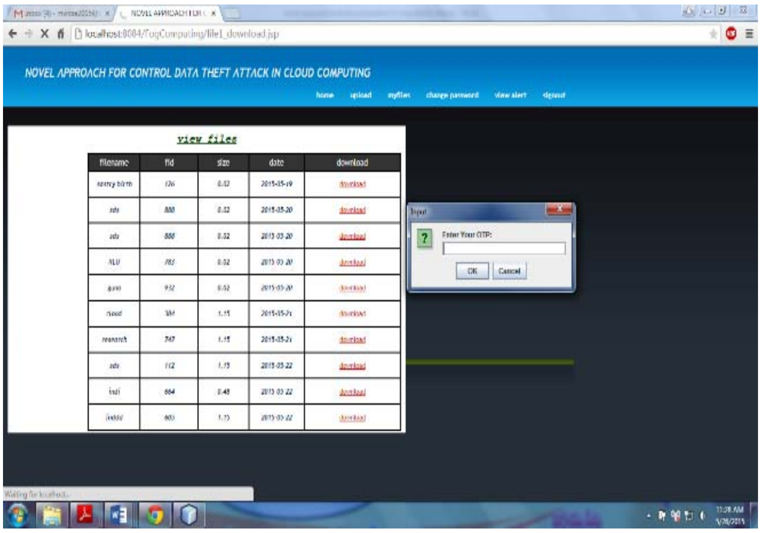
NOVEL APPROACH FOR CONTROL DATA THEFT ATTACK IN CLOUD COMPUTING

view files

your login access time 05:00:00 to 06:00:00

filename	fid	size	date	download
sastry birch	126	0.02	2015-05-19	click here
sds	888	0.02	2015-05-20	click here
sds	888	0.02	2015-05-20	click here
KLU	783	0.02	2015-05-20	click here
gune	932	0.02	2015-05-20	click here
cloud	384	1.15	2015-05-21	click here
research	747	1.15	2015-05-21	click here
sds	112	1.15	2015-05-22	click here
indi	664	0.48	2015-05-22	click here
indddd	605	1.15	2015-05-22	click here

Figure 7. Files in cloud



NOVEL APPROACH FOR CONTROL DATA THEFT ATTACK IN CLOUD COMPUTING

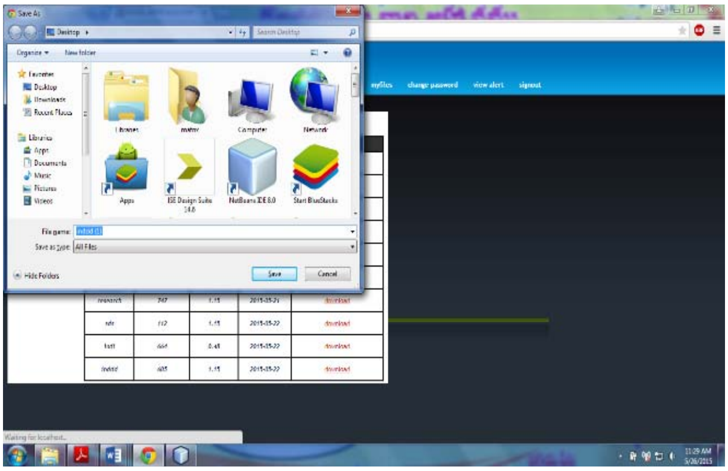
view files

filename	fid	size	date	download
sastry birch	126	0.02	2015-05-19	download
sds	888	0.02	2015-05-20	download
sds	888	0.02	2015-05-20	download
KLU	783	0.02	2015-05-20	download
gune	932	0.02	2015-05-20	download
cloud	384	1.15	2015-05-21	download
research	747	1.15	2015-05-21	download
sds	112	1.15	2015-05-22	download
indi	664	0.48	2015-05-22	download
indddd	605	1.15	2015-05-22	download

Enter Your OTP:

Waiting for localhost...

Figure 8. OTP Verification



File name: indddd (1)

Save as type: All Files

research	747	1.15	2015-05-21	download
sds	112	1.15	2015-05-22	download
indi	664	0.48	2015-05-22	download
indddd	605	1.15	2015-05-22	download

Waiting for localhost...

Figure 9. Downloading Data

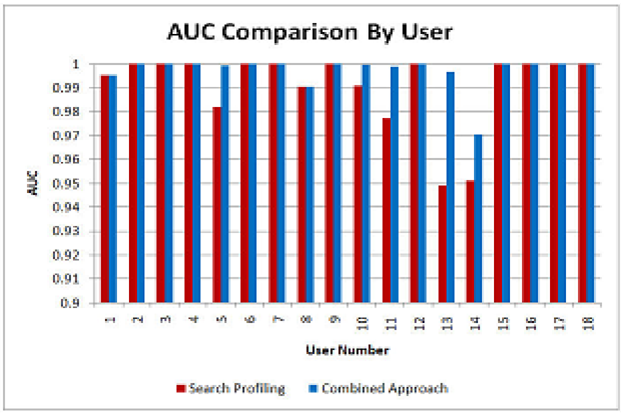


Figure 10. Results

This results can be used for identify the unauthorized access by analyzing user profiles[8] [9]. If any unauthorized profile is identified by presenting the challenging question if he is answered the original data is displayed otherwise large amounts of decoy data is displayed. The decoy information is stored in a local server, whenever it required it will retrieved from server. The detector is continuously monitoring usage of accessed file and search criteria of files.

7. CONCLUSION

We implemented a different approach for securing personal and business data in the cloud. We propose a system to prevent data access patterns by profiling user behavior to establish if and when a wicked insider criminally accesses someone documents in the cloud services. The decoy technology allows the use to keep decoy information or dummy information in the file system to mislead insider data theft attackers. We would like to increase the user profile management and use more decoy information from various domains for civilizing exact positives of the fog computing.

REFERENCES

[1] Ben-Salem M, Salvatore J. Stolfo, and Angelos D. Keromytis, “Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud,” *IEEE symposium on security and privacy workshop (SPW)*, 2012.

[2] Saif Ali Abd., Alradha Alsaidi, “Protect Sensitive Data in Public Cloud from an Theft Attack and detect Abnormal Client Behavior”, *In IJESC,* 2014.

[3] Gunasekhar T., Rao K. T., Basu M. T., "Understanding insider attack problem and scope in cloud," *Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on*, pp. 1-6, 2015.

[4] Sayaliraje, Namratapatil, Shitalmundhe, and Ritikamahajan “Cloud security using fog computing”, *Proceedings of IRF International Conference,* 2014.

[5] V. Sriharsha, V. Prabhaker, and N. Krishna Chythanya, “Dynamic Decoy File Usage to Protect from malicious insider for data on public cloud”, *International Journal of Advanced Engineering and Global Technology*, Vol. 1, No. 3, 2013.

[6] P. Jyothi, R. Anuradha, and Dr. Y. Vijayalata, “Minimizing Internal Data Theft in Cloud Through Disinformation Attacks”, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, No. 9, 2013.

[7] Dnyanesh S. Patil, Suyash S. Patil, Deepak P. Pote, and Nilesh V. Koli, “Secured cloud computing with decoy documents”, *Proceedings of 4th IRF International Conference,* Pune, 2014.

[8] Madhusri K. Navneet, “Fog Computing: Detecting Malicious Attacks in a cloud”, *International Journal of Scientific & Engineering, Research,* Vol. 4, No. 5, 2013.

[9] Gunasekhar T., *et al.*, "A Survey on Denial of Service Attacks", *International Journal of Computer Science and Information Technologies,* Vol. 5, No. 2, pp. 2373-2376, 2014.

[10] Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” 2010.

[11] Gunasekhar T., *et al.*, "Mitigation of Insider Attacks through Multi-Cloud", *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 5, No.1, pp. 136-141, 2015.

[12] M Dileep Kumar, M. Trinath Basu, T. Gunasekhar, ”Meshing VANEMO protocol into VANETs”, *International Journal of Applied Engineering Research,* Vol. 10, No. 12, pp. 31951-31958, 2015.

[13] Anusha M., Vemuru S., and Gunasekhar T., "TDMA-based MAC protocols for scheduling channel allocation in multi-channel wireless mesh networks using cognitive radio", *Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on*, pp. 1-5, 2015.

[14] T. Gunasekhar, K. Thirupathi Rao, ”EBCM: Single Encryption, Multiple Decryptions”, *International Journal of Applied Engineering Research*, Vol. 9, No. 19, pp. 5885-5893, 2014.

[15] R. Praveen Kumar, Jagdish Babu, T. Gunasekhar, and S. Bharath Bhushan, ”Mitigating Application DDoS Attacks using Random Port Hopping Technique”, *International Journal of Emerging Research in Management &Technology,* Vol. 4, No. 1, pp. 1-4, 2015.

[16] Anusha M., Srikanth Vemuru, and T. Gunasekhar, "Transmission protocols in Cognitive Radio Mesh Networks" *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 5, No. 4, 2015.

BIOGRAPHIES OF AUTHORS

K. Narasimha Sastry, received MCA degree from KLUniversity, Guntur, A.P in 2010 and pursuing M.Tech degree in Computer Science &Engineering at KLUniversity.

Dr B. Thirumala Rao, Professor PhD. He had published research papers at National andInternational Journals and Conferences. Currently he is working has Professor at KL University Vijayawada.

T.Gunasekhar received his Bachelor of Technology and Master of Technology from Jawaharlal Nehru Technological University Anantapur in 2011 and 2013 respectively.He is currently pursuing PhD at K L University.