International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-7)

Research Article | **July 2014**

Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication

Harpreet Singh
Research Scholar,
Department Of Computer Science Engineering,
Chandigarh Engineering College,
Landran, India

Er. Gagandeep Singh
Assistant Professor,
Department Of Computer Science Engineering,
Chandigarh Engineering College,
Landran, India

Er Madhu Bahl
Assistant Professor,
Department of Computer Science Engineering,
Chandigarh Engineering College,
Landran, India

Abstract—

Outsourcing the data in cloud computing is exponentially generating to scale up the hardware and software resources. However, outsourcing the data to a third party causes the security and privacy issues to become a critical concern. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. In this paper the authors propose and later implement private and public cloud, where the private cloud should store only the organization's sensitive structure information such as the key management services and user membership information, and the public cloud should store the actual data in the cipher-text form by using an encryption algorithm where every individual multimedia file will be encrypted using different keys which will be later decrypted by dynamically generating keys at the time of accessing multimedia from Public Cloud.

Keywords-Outsourcing,unauthorized,Encryption, Private, Public, Cipher.

I. INTRODUCTION

There has been a growing trend in the recent times to store data in the cloud with the dramatic increase in the amount of digital information or store archival data. Cloud data storage can be particularly attractive for users with unpredictable storage demands, requiring an inexpensive storage tier or a low-cost, long-term archive. By outsourcing user's data to the cloud, service providers can focus more on the design of functions to improve user experience of their services without worrying about resources to store the growing amount of data. Cloud can also provide on demand resources for storage which can help service providers to reduce their maintenance costs. Furthermore, cloud storage can provide a flexible and convenient way for users to access their data from anywhere on any device.

The most cited definition of cloud computing is the one proposed by the US National Institute of Standards and Technology (NIST). NIST provides the following definition [1]: "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Along with the widespread enthusiasm on cloud computing, however, concerns on data security with cloud storage are arising due to unreliability of the service and malicious attacks from hackers. Recently more and more events on cloud service outage or server corruption with major cloud infrastructure providers are reported [2–5]. Data breaches of noteworthy cloud services also appear from time to time [6-8]. Besides, the cloud service providers may also voluntarily examine customers' data for various motivations. Therefore, we argue that the cloud is intrinsically neither secure nor reliable from the view point of the cloud customers. Without providing strong security, privacy and reliability guarantee, it would be hard to expect cloud customers to turn over control of their data to cloud servers solely based on economic savings and service flexibility. To address these concerns and thus motivate the wide adoption of data outsourcing in cloud, in this paper the authors will explore the problem of secure and reliable data outsourcing. Cloud has several security issues involving assurance and confidentiality of data [9]. A user entrusting a cloud provider may lose access to his data temporarily or permanently due to an unlikely event such as a malware attack or network outage. On April 21, 2011, EC2's northern Virginia data center was affected by an outage and brought several websites down [10, 11]. Problems caused by this outage lasted till April 25, 2011 [10]. Such an unlikely event can do significant harm to the users. Confidentiality of user data in the cloud is another big concern. Cloud has been giving providers an opportunity to analyze user data for a long time. In addition, outside attackers who manage to get access to the cloud can also analyze data and violate user privacy. Cloud is not only a source of massive static data, but also a provider of high processing capacity at low cost. This makes cloud more vulnerable as attackers can use the raw processing power of cloud to analyze data [12]. Security issues have been the dominate barrier of the development and widespread use of cloud computing. There are three main challenges for building a secure and trustworthy cloud system:

• **Outsourcing** – Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues,

© 2014, IJERMT All Rights Reserved

first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owners' control.

• **Multi-tenancy** – Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Moreover, in a virtualized environment, data belonging to different customers may be placed on the same physical machine by certain resource allocation policy. Adversaries who may also be legitimate cloud customers may exploit the co-residence issue. A series of security issues such as data breach [13], [14], [15], computation breach [13], flooding attack [16], etc., are incurred. Although Multi-tenancy is a definite choice of cloud venders due to its economic efficiency, it provides new vulnerabilities to the cloud platform. Without changing the multi-tenancy paradigm, it is imperative to design new security mechanisms to deal with the potential risks.

• **Massive data and intense computation** – cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.
The remainder of the paper is organized as follows. Section II discusses the related work. In Section III, the authors describe assumptions on which this research article rely and tried to fill the gap in the later sections. Section IV presents the details and the flow of the major work to be covered in this architecture. The authors introduce the construction of the new cloud security model and architecture with two tier encryption. In Section V, the authors provide implementation of the proposed architecture. In Section VI the authors discuss results and comparison study of implemented architecture with other models. Finally, Section VII discusses future extensions and concludes the paper.

II. LITERATURE REVIEW

Security in cloud is one of the major areas of research. The survey shows that, the researchers are focusing on efficient algorithms and encryption techniques to enhance the data security in cloud. Brian Hay et.al[17] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies and digital forensics. In operational trust modes, the encrypted
communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data. The issues are clarified using the digital forensics techniques namely the ephemeral nature of cloud resources and seizing a "system" for examination. John C. Mace et.al [18] have proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions. Service oriented architecture (SOA) is used for work flow deployment in an enterprise. For efficiency, productivity and to achieve public cloud, the cloud computing uses the approaches like retaining control, setting policy, monitoring and runtime security. The dynamic deployment approaches in public cloud computing are security assessment, work flow deployment, policy assignment, audit data and policy analysis. Qiang Guoet.al [19] gives the unique definition for trust in cloud computing and various issues related to trust are discussed here. An extensible trust evaluation model named ETEC has been proposed which includes a time-variant comprehensive evaluation method for expressing direct trust and a space variant evaluation property for calculating recommendation trust. An algorithm based on ETEC model is also shown here. This model also calculates the trust degree very effectively and reasonably in cloud computing environments. Other approaches to protect data privacy in a cloud environment include using direct encryption and proxy re-encryption. In these cryptographic schemes, data is allowed to be encrypted directly to the users with whom the owners wish to share the data [20], [21].
Jing-Jang Hwang et al. [22], has proposed a business model for cloud computing for data security using data encryption and decryption algorithms. In this method cloud service provider has responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for process of data in cloud server. The main disadvantage of this method is, there is no control of data for data owner i. e, data owner has completely trusted with cloud service provider and he has more computational overhead. Junzuo et al. [23], proposed an Attribute Based Encryption (ABE) and verifiable data decryption method to provide data security in cloud based system. They have been designed the data decryption algorithm based on the user requested attributes of the out sourced encrypted data. One of the main efficiency drawbacks of this method is, cloud service provider has more computational and storage overhead for verification of user attributes with the outsourced encrypted data. While introducing third party auditor we can reduces the storage, computation, and communication overheads of the cloud server, which improves the efficiency of the cloud data storage. Fatemi Moghaddam et al. in [24], discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing environment. They have proposed two separate cloud servers; one for data server and other for key cloud server and the data encryption and decryption process at the client side. The main drawback of this method is to maintaining two separate servers for data security in cloud, which creates a more storage and computation overheads.

© 2014, IJERMT All Rights Reserved

III. PROBLEM FORMULATION

The existing frameworks proposed so far focuses only on securing the data stored either on the distributed servers or local servers interacting with cloud through interfaces or agents. The use of either applying the encryption algorithms or putting the authentication mechanism in place alone cannot help to protect the data from the unauthorized access keeping in view the present robust attacking models. So the need is to suggest such a mechanism where encryption of the content, authorization of user as well the delivery of content to end terminals has been considered.

In a public cloud, as data can be stored in distributed data centers; there may not be a single central authority which controls all the data centers. Furthermore the administrators of the cloud provider themselves would be able to access the data if it is stored in plain format. Hence there is a need of enhancing data security by employing cryptographic techniques to encrypt data from misuse together with some authentication mechanism by which virtue of which the privacy and security of cloud can be achieved on one end and mass data storage feature of public clouds on other end.

IV. PROPOSED 2- WAY AUTHENTICATION MODEL

In this proposed model the authors will explore the ways to enhance the security of multimedia content using hybrid algorithms while being delivered to their end users. The security frame work will take care of authorization and authentication of user while accessing any cloud server. The hybrid encryption mechanism will make the storage and transmission secure by associating some payloads defining the minimum required security parameters. The robustness of this delivery mechanism will cover the multimedia streaming over CDC, caching the media content onto the edge server from storage cloud and will be used to minimize the latency of content delivery. The overall scenario will outline architecture for designing and deployment of Applications with rich multimedia content over cloud servers as SAAS and also taking the advantage of blob storage of clouds like Windows azure.

In the proposed system the authors are making the system more secure by adding two-way authentication for validating any user for data access. Here first user will be validated for username and password and then later validated in terms of secret key which is already mailed in the mailing account of that user. Moreover in this proposed model the authors will add the subscriptions for users based on their paid memberships. On the basis of this feature the user can access the data with different allocated bandwidths and the different amount of data.

The major outcomes to be achieved in this proposed work are:

- The proposed work is assumed to develop hybrid private cloud and public cloud, where the private cloud should store only the organization's sensitive structure information such as the key management services and user membership information, and the public cloud should store the actual data in the cipher-text form by using any existing encryption algorithm. This proposed architecture not only will dispel the organization's concerns about risks of leaking sensitive structure information, but will also takes full advantage of public cloud's power to securely store large volume of data.

- In Proposed work all data on public cloud is stored in encrypted form by employing cryptographic techniques which will save data from misuse from cloud service providers and restrict data access to only those intended by the data owners.

- In Proposed Mode, the user is validated using the two authentication mechanism .First the user is authenticated in terms of username and password combination in 3 attempts and then secret key is used for decrypting the original data back into the plain text form. This level two authentication is to be done on per session basis.

- In proposed architecture, User creation will be further made strong by adding premium memberships which will help users to use multimedia resources differently and under different network bandwidths.

- In proposed model while imposing cryptographic techniques, a feature of constant key size needs to be added. Also Revoking User should not affect other users and key management in this architecture.

All these features are summed up in the following flow based figure 1.

V. IMPLEMENTATION

The authors have implemented the model of 2- way authentication based on Public Cloud. The system is implemented in MVC Framework. Later this implemented web model is hosted on Microsoft's Azure cloud platform where the cloud use SQL database for its main storage of table contents which is to be stored on private cloud within an organization. Next the authors uploaded the data on this third party Public Cloud via implemented interface for 2-Way authentication cloud architecture for whose storage the authors created a storage account on Microsoft Azure Platform. Finally the authors allowed users to make access of this already stored data on Microsoft Azure cloud via this implemented model using two tier encryption service based on the GUID service of .NET platform.

The authors have performed experiments on a machine with Intel(R) Core (TM) i3-2310M CPU @ 2.10 GHz 2.10 GHz processor, 3 GB of RAM and Microsoft Windows 7 Ultimate 32 bit Operating System. Once the administrator of this implemented architecture makes successful login, then s/he will be redirected to the main interface of this architecture where s/he can now go for the creation of user base for the system and then impose permissions on these created users.

© 2014, IJERMT All Rights Reserved

Next the administrator will upload the data content which is to be stored in storage account already created on Windows Azure Cloud. Here this data is first encrypted using the GUID service provided by the .NET platform by virtue of which an alpha numeric key is to be generated for every file. Once the file gets encrypted, this key is to be stored on the private Cloud. Although the private cloud is lying within the reach of an organization but for further security, this key is further encrypted into cipher text form by applying AES algorithm. Here the cipher texted key is stored on private cloud and new generated key is also stored in terms of new record on database. Now authentic users can make login to this architecture to access the stored data on Microsoft Azure Cloud Storage account. Here if any unknown user will try to access this web interface and validation fails, then s/he can be warned in several attempts to go for authentic details and then in next attempt s/he can be blocked for some time specific time interval to be decided by the administrator. This is the added security mechanism in this architecture which will enhance the security mechanism for accessing the implemented architecture. Once making successful login the users can access and download the stored content on Cloud based on their permissions and restrictions imposed on them which were initially decided in admin interfaces of the architecture. For downloading every data file on cloud, the user will get a secret key of AES on his or her mailbox which s/he needs to provide for decrypting the data .Once the key is submitted, this key is matched with the secret key in database and if matched the original key will be decrypted and by virtue of which a message box will be provided to user for accessing the corresponding data file.

VI. RESULTS AND COMPARATIVE ANALYSIS

In this implemented architecture model, the authors have successfully added the two tier encryption technique for providing security on public cloud. The data uploaded on the cloud server is first converted into cipher text. For decrypting the data on the receiving end, every time the file is accessed, it needs to be decrypted with the secret key which is already provided to the user in mailbox. In comparison to other cryptographic and security models, our architecture added the power to the existing models in terms of constant cipher text, no re-encryption after revocation of users and extended the encryption to two tiers. In this system architecture, the cipher text remains constant irrespective of varying the user base for the system. Moreover there is no need of re-encryption in key management after some of the users are deleted from the system or denied the access of the system. Also the key for encrypting the file is further re-encrypted in this model to make this model more secure in terms of attacks and thus extending the cryptographic mechanism to two tiers.

The experimental study of this system proved this architecture to be better in terms of constraints and the performance comparison of every activity to be shown as well in terms of the following line chart:

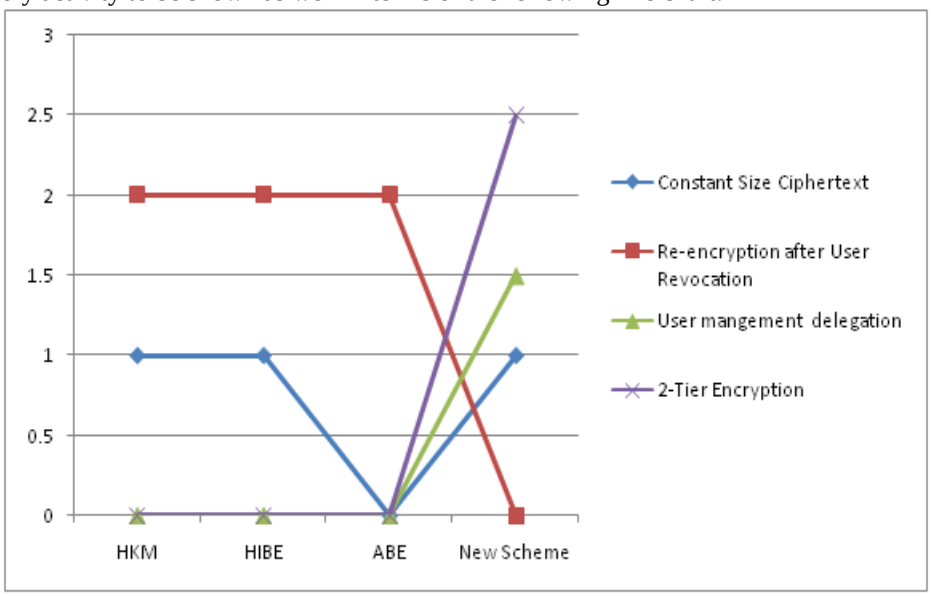

Fig 2 Performance comparisons in various models with our new Scheme

Clearly this new model shows improvement in all elements of constant cipher text, re-encryption on user revocation and two tier encryption.

VII. CONCLUSION

In this paper, first the authors proposed a new architecture for cloud data storage in which the private cloud should store only the organization's sensitive structure information and the public cloud should store the actual data in the cipher-text form by using newly designed encryption algorithm. The cryptographic algorithm will work on individual multimedia files for which every time the user will have to dynamically decrypt by using different keys. Moreover the authors have proposed and implemented the two tier encryption mechanism for this architecture which will greatly enhance the security of the proposed architecture. The authors believe that the implemented system has the potential to be useful in commercial situations as it captures practical access policies in a flexible manner and provides secure data storage in the cloud enforcing these access policies.

© 2014, IJERMT All Rights Reserved

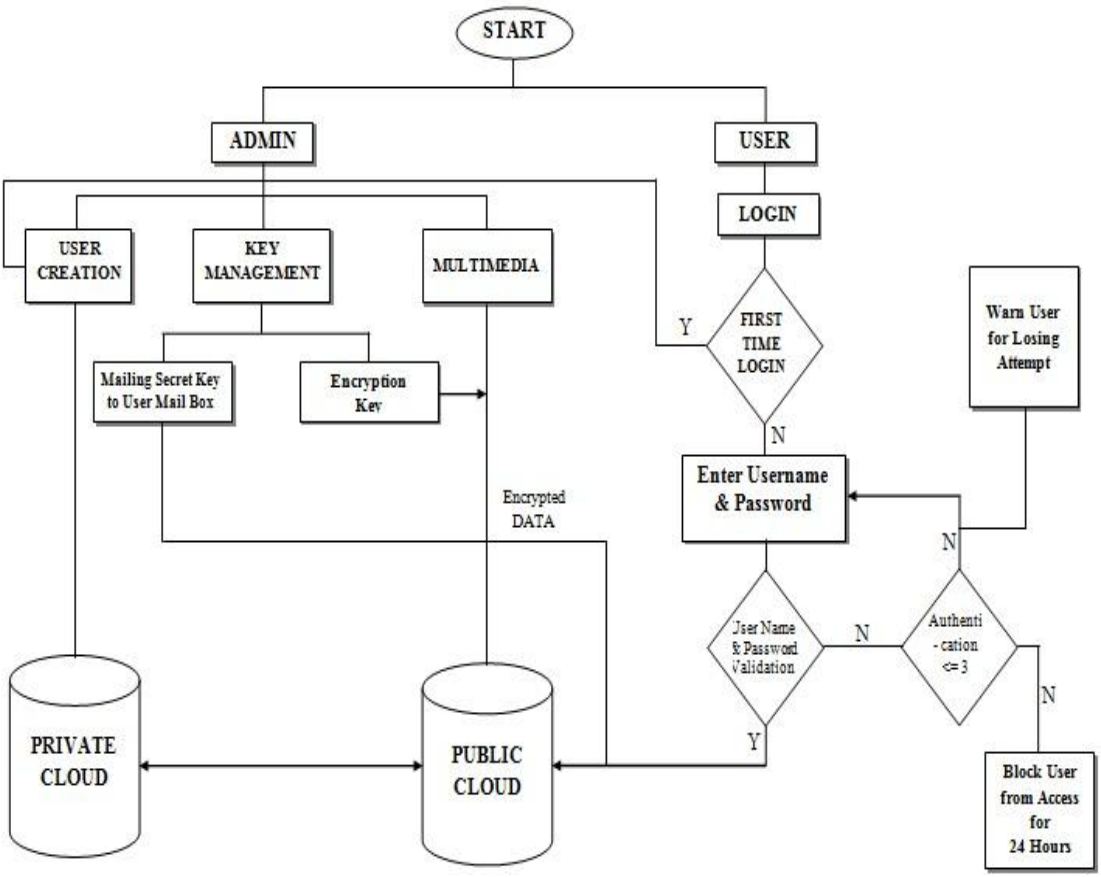

Figure 1 Two-way authentication based Cryptographic model for Secure Data Storage

REFERENCES

[1] P.Mell and T. Grance, "The NIST Definition of Cloud Computing", [2011].
[2] Blog service hosted by google crashes review.http://hostwisely.com/blog/blog-service-hosted-by-google-crashes.
[3] Microsoft cloud data breach heralds things to come. http://www.techworld.com.au/article/372111
[4] Summary of the amazon ec2 and amazon rds service disruption in the us east region.http://aws.amazon.com/message/65648
[5] Zack Whittaker. Amazon web services suffers partial outage. http://www.zdnet.com/blog/btl/amazon-web-services-suffers-partial-outage/79981
[6] Mathew J. Schwartz. 6 worst data breaches of 2011, [2011]. http://www.informationweek.com/news/security/attacks/232301079
[7] Aaron Souppouris. Linkedin investigating reports that 6.46 million hashed passwords have leaked online, [2012]. http://www.theverge.com/2012/6/6/3067523/linkedin-password-leak-online.
[8] Darlene Storm. Epsilon breach: hack of the century? [2011]. http://blogs.computerworld.com/18079/epsilon_breach_hack_of_the_century.
[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "Above the clouds: A berkeley view of cloud computing, Technical report, EECS Department, University of California, Berkeley", [2009].
[10] Wikipedia. Amazon elastic compute cloud- Wikipedia, the free encyclopedia, [2012].
[11] Amazon Web Services: Overview of Security Processes, May [2011].
[12] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. "Controlling data in the cloud: Outsourcing computation without outsourcing control", pages 85–90, [2009].
[13] Google Docs experienced data breach during March 2009. http://blogs.wsj.com/
[14] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", Proc. 16th ACM conference on Computer and communications security, pp. 199-212, [2009]
[15] N. Santos, K.P. Gummadi, and R. Rodrigues,"Towards trusted cloud computing", Proc. conference on Hot topics in cloud computing,[2009].
[16] C. Dovrolis, P. Ramanathan, and D. Moore, "What do packet dispersion techniques measure?" In Proc. IEEE INFOCOM, pp. 905-914, [2001].
[17] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, [2011].

© 2014, IJERMT All Rights Reserved

[18] John C.Mace, Aad van Moorsel, Paul Watson, "The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments" School of Computing Science & Centre for Cybercrime and Computer Security (CCCS) Newcastle University, Newcastle upon Tyne, NE1 7RU, UK.

[19] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments" School of lnformation Science and Engineering, Northeastern University, Shenyang, P.R. China, Computing Center, Northeastern University, Shenyang, P.R. China, 2011 3rd International Conference on Advanced Computer Control ,[2011].

[20] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "SiRiUS: Securing remote untrusted storage", in Proc. NDSS, pp. 1–15 ,[2003].

[21] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved proxy re-encryption schemes with applications to secure distributed storage" ,in Proc. NDSS, pp. 29–43 Feb.

[22] Jing-Jang Hwang, Taoyuan, Taiwan,Yi-Chang Hsu, Chien-Hsing Wu, A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, in International Conference on Information Science and Applications (ICISA), pages 1-7, [2011].

[23] Junzuo Lai, Deng R H, Chaowen Guan, JianWeng, Attribute Based Encryption with Verifiable Outsourced Decryption, *in* IEEE Transactions on Information Forensics and Security, vol. 8(8), pages 1343-1354, [2013].

[24] Fatemi Moghaddam F,KarimiO, Alrashdan M T, A Comparative Studyof Applying Real-Time Encryptionin Cloud Computing Environments, in IEEE 2nd International Conference on Cloud Networking, pages 185-189, [2013].

© 2014, IJERMT All Rights Reserved