Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

OneTK: Key Distribution Center at Cloud Providers towards End to End, Security the Services through Session Keys & alerts

J. Purna Prakash[1], M. Rama Raju[2], P.Avaniketh[3]

[1,2,3] Computer Science & Engineering, Christu Jyoti Institute of Technology & Science

Abstract-- Using End to End Connection in packet Switching networks for providing higher security in Cloud Computing. In cloud computing a major role is provide security to services that may be PaaS(Platform as a Service), SaaS(Software as a Service) , CaaS(Communication as a Service) , IaaS(Infrastructure as a Services) , MaaS (Monitoring as a Service)n, XaaS(X: Platform, Software, Monitoring, Infrastructure). Cloud computing provides wide range of services. Large, Small and medium businesses are depending on out sourcing of data services and computation on cloud this is mainly deals with SaaS. The cloud provides a very high efficient service for the business organizations. These business organizations trust cloud service providers on their data security. But providing security is highly risk in cloud through the third party, especially in private cloud services. Existing data security methods are not so effective. By using this End to End Connection and Session Keys and attempts is to be covered secularism in the area of Cloud computing users.

A new approach for securing the data from cloud. OTK – "One Time Key Distribution File" is a service that protects unauthorized file downloading form the cloud.

Keywords: Cloud Services, Cloud security, KDC: Key Distribution Center, End to End, Session Keys.

I. INTRODUCTION

In Cloud Computing Various Businesses can be proved, especially startups, small and medium businesses (SMBs), are opting for outsourcing data and computation to the Cloud for their data storage. This provides operational efficiency, but comes with greater risks, perhaps the most serious of which are data theft attacks.

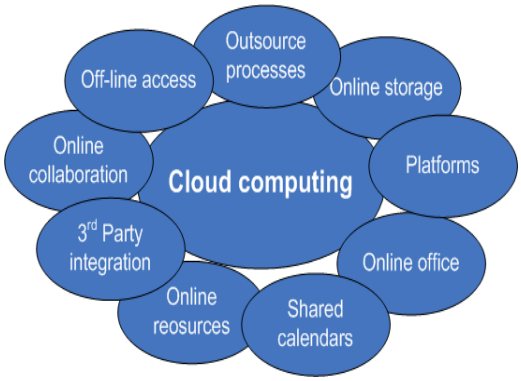

Figure 1. Various Services under cloud computing

Threat of a malicious insider [1] is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain under cloud providers with third party, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it

analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary ranging from the hobbyist unauthorized person, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. Level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

Recent Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website TechCrunch [2], [3], and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed [4], [5]. The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents, hosted on Google's infrastructure as Google Docs. The damage was significant both for Twitter and for its customers.

While this particular attack was launched by an outsider, stealing a customer's admin passwords is much easier if perpetrated by a malicious insider. Rocha and Correia outline how easy passwords may be stolen by a malicious insider of the Cloud service provider [6]. The authors also demonstrated how Cloud customers' private keys might be stolen, and how their confidential data might be extracted from a hard disk. After stealing a customer's password and private key, the malicious insider get access to all customer data, while the customer has no means of detecting this unauthorized access.

Hence by avoiding such type of attacks the third party has to be must maintained for OTK in case of any information being processed. Through the network with the maximum access with OTK for third party admin, providers admin and users.

Key management: The key management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

The Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. Than Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements.

Private cloud - Private cloud, the infrastructure is provisioned solely for a single organization, and may be managed internally or by a third-party and hosted externally (virtual private cloud). Also in a private cloud, multiple business units can be separated by multi- tenants and the provider has full knowledge of resource locations as they own the infrastructure.

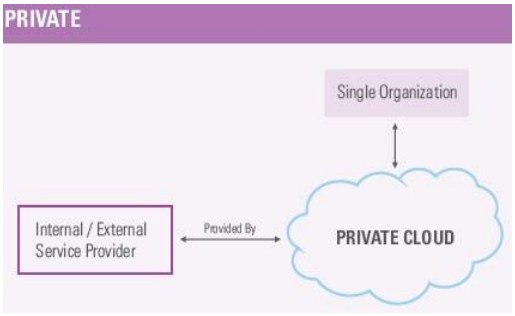

Figure 2. Private cloud scenario

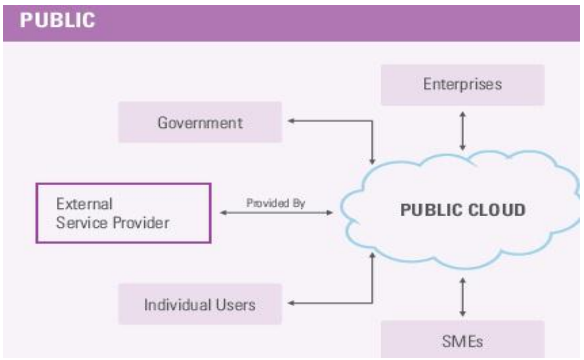

Figure 3. Public Cloud Scenario

Public cloud - Public cloud, the cloud infrastructure is provisioned by the cloud provider for open use by the any type of customer. The infrastructure may be owned, managed, and operated by a business, academic, or government organization, or some combination of these entities.

Hybrid cloud - A hybrid cloud is composed of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. A hybrid cloud can also consist of multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

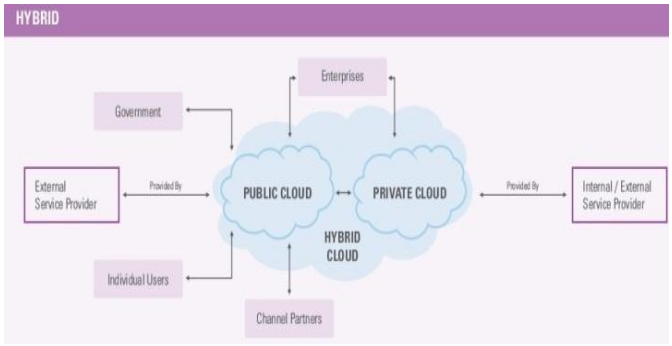

Figure 4. Hybrid Cloud

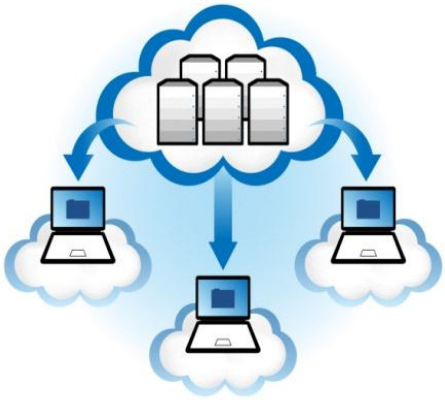

Figure 5. Services availability

Service availability - Various Services available in cloud computing towards access information in accessing the data while coming to services which can be utilized in cloud users. Each every cloud is provided through the third party hence there the services can be protected by the trusted third party than only the data can be accessed in a secure manner while in the end user access the data.

II. SECURING CLOUD WITH OTK

Main service of cloud is to store documents; media files etc. cloud provides public cloud and private cloud. When the files are stored in public cloud such files will not have security as they can be downloaded by the any user in organization. Private cloud need to provide much higher security for the users that the user stored files can be accessed by only that user. Unauthorized using of files must be detected and avoided in the private cloud.

Cloud providers and user problem of providing security of confidential information remains a core security problem that, to date has not provided the levels of assurance most people desire. Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls. One needs to prepare for such accidents.

Basic idea of OTK is to avoid unauthorized access of file or documents stored in private cloud. Every user will be registered with cloud service provider. Each user will have a user login id and password for his access. Some old methods require to get permission from third party to get session keys to communicate towards through the cloud providers and users in correspondence to the third party.

By using OTK login id, password with session key files are enough to access file in private cloud storage. While registration of user we in cloud we ask him to register his Personal data. This personal data is validated by a random generated with session keys to generate 4 digit number which will be sent as a SMS to that mobile as well as company E-mail id.

Once user mobile and E- mail id is registered with his user cloud account the services that enable to provide alert service. Whoever logs in cloud with some login id and password immediately an alert message will be sent to original user's registered mobile as well as Email - id. If original user logged in, cloud data services will don't have any security risk.

Figure 6 Alerts information

If any unauthorized persons logs in immediately original user can know that his account is being hacked he can block it.

For the file and documents access, when the user requests it, that file will not be downloaded immediately. A randomly generated session keys and4 digit code will be sent as OTK to registered mobile or Email id. If that 4 digit code entered correctly the only file access is allowed if not file access is denied.

SMS service provider. Mobile SMS service provider should be able to send SMS to registered mobiles as fast as possible without fail, so that we can provide a high security to private cloud. We can allow the user to change his registered mobile number with authentication.

In the cloud data storage, a user stores his data through the cloud service provider into a set of the cloud servers. The cloud servers run on the distributed system. Data redundancy can be applied with technique of erasure correcting code to further tolerate faults or server crash as users grows in size. By using application, the user interacts with cloud server via cloud service provider to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations are considering are block revise, erase, insert and affix [3].

As above mentioned diagram the security problem occurs in third party to user access through cloud server regarding this at the end user access we have to implement different aspects to use our existed algorithms in effective. A normal small company can use high level data secure methods by using large keys towards in algorithms. The algorithms limitations will be taken place again do to in excellent manner. Whereas earlier if we want to use algorithms like this there is problem of using processing capabilities to encrypt our data.

Design Goals

To make sure the security and dependability for data storage in cloud under the aforementioned antagonist model, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

I. Storage accuracy: to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.

II. Fast access of user: to effectively locate the mal- functioning server when data access has been detected.

Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, erase or affix their data files in the cloud.

III. OTK WORKING IN CLOUD COMPUTING

The main aim to work OTK to within the specific time the third party is going to generate through confirmation if any problem occurs, especially when IP address fails due to assigning some other IP

address to the organization there is problem of getting authentication. Than introducing the high secure concept as key is distributed among various session key files towards access the data in secure manner also distribution can be handle in secure manner while accessing the data. Here initially the request has made to the third party to get access with the cloud providers to access information. Symmetric schemes require both parties to share a common secret key towards the mobile and Email ids. Nothing but public keys. To generate session keys from third party we require public key schemes to acquire valid public keys

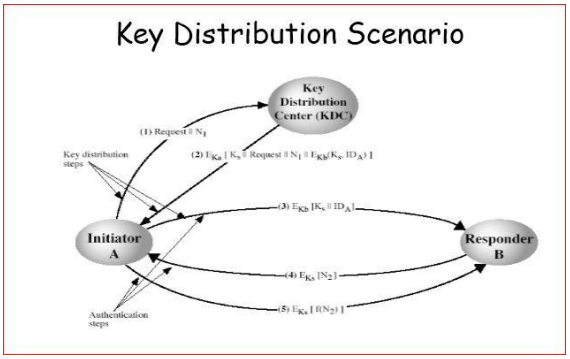

Figure 8. Key Distribution Scenario in Cloud computing

In above Scenario Users who are using cloud services initially they get permission for accessing data from cloud providers. Than the Third party has to generate a session key towards access the data from cloud providers and users. By its utilization of keys the key is provided to the user to communicate with cloud providers with corresponding sessions. Than with key only the cloud users can communicate with cloud providers towards using the alert message to the mobile phone and Email id.

IV. DATA CENTER

Data center will provide various utilities like Software as a Service, Network Security, and Virtualization Etc. Hence by using data center as a service with the utilization of service through the alerts in various methods like messaging with sending alerts to the mobile and so on. By providing more and more secure to the cloud towards beneficiary to the both side to avoid unauthorized persons including working under organization with the small position employees to access to authenticate data.

Figure 9. Data Center

a) End use access in Location of Encryption Devices only

As we in paper we giving security to wards in end to end connection. With end-to-end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The data, in encrypted form, are then transmitted unaltered across the network to the destination terminal or host. The destination shares a key with the source and so is able to decrypt the data. This approach would seem to secure the transmission against attacks on the network links or switches.

There is, however, still a weak spot.

Consider the following situation. A host connects to an X25 packet-switching network, sets up a virtual circuit to another host, and is prepared to transfer data to that other host using end-to-end encryption. Data are transmitted over such a network in the form of packets, consisting of a header and some user data. What part of each packet will the host encrypt? Suppose that the host encrypts the entire packet, including the header. This will not work because, remember, only the other host can perform the decryption. The packet-switching node will receive an encrypted packet and be unable to read the header. Therefore, it will not be able to route the packet. It follows that the host may only encrypt the user data portion of the packet and must leave the header in the clear, so that it can be read by the network.

Thus, with end-to-end encryption, the user data are secure. However, the traffic pattern is not, because packet headers are transmitted in the clear. To achieve greater security, both link and end-to-end encryption are needed, as is shown in

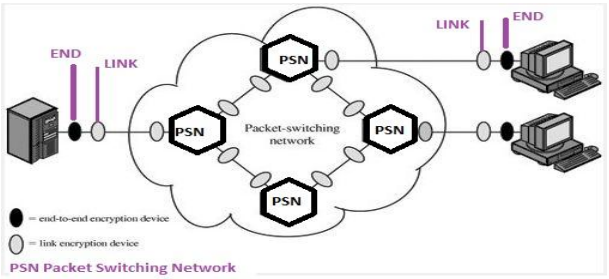

Figure 10. Encryption across a Packet-Switching Network

To summarize, when both forms are employed, the host encrypts the user data portion of a packet using an end-to-end encryption key. The entire packet is then encrypted using a link encryption key. As the packet traverses the network, each switch decrypts the packet using a link encryption key to read the header and then encrypts the entire packet again for sending it out on the next link. Now the entire packet is secure except for the time that the packet is actually in the memory of a packet switch, at which time the packet header is in the clear.

In This Process While Encryption the data the user must registered with session Id in corresponding to the time and attempts within the specific amounts time the users as to access and use those services. Requesting downloading and getting the alerts to mobile and everything maintain history form in addition to IP address where that specific Class are using in our method with specific range. Hence this gives more and more security with referred with end to end connection and entering one time key at the end use sides

V. CONCLUSION

In this paper propose a new novel approach for securing the data from any cloud. OTK – "One Time Key Distribution File" is a service that protects unauthorized file downloading or accessing form the any cloud. Unauthorized user account access and file access will be detected. An alert message and OTK can be sent to original user mobile and Email Id. So that theft attacks can be avoided in private cloud. Mainly the user has to get session keys from third party to generate request within the session period the communication is possible.

VI. FUTURE WORK

Providing data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As in Cloud computing providing protection force to our services a big challenge. In addition we can link to the work towards secure patterns connection to the mobile phones as well as for Email connections we can use some pattern or thumb techniques to provide more dynamic security for cloud users and providers.

VII. ACKNOWLEDGEMENTS

I thank my students who have implemented the extension part of this paper under my guidance Also, I would like to thank the management (Rev. Fr. Y. PapiReddy , the director), Principal (Dr.J.B.V.Subrahmanyam) for providing this opportunity and for their constant encouragement and also to HOD A. Poorna chander reddy who motivate and suggest few concepts towards publishing the paper. I also thank CSE Staff M. Vjiay kumar and T. Prakash helping to designing the Pictures and hardware for technical support in this paper.

REFERENCES

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[2] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online].Available:http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitter-documents/
[3] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [On-line]. Available: http://venturebeat.com/2010/03/24/french-hacker-who-leaked-twitter-documents-to-techcrunch-is-busted/
[4] D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online].Available:http://www.zdnet.com/blog/security/french-hacker-gains-access-to-twitters-admin-panel/3292
[5] P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010.[Online].Available:http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html
[6] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual ComputingEnvironments, Hong Kong, ser. DCDV '11, June 2011.
[7] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–8. [Online].Available:http://dl.acm.org/citation.cfm?id=1924931.1924934
[8] *Fog Computing:* Mitigating Insider Data Theft Attacks in the Cloud.[Online].Available:http://ids.cs.columbia.edu/sites/default/files/Fog_Computing_Position_Paper_WRIT_2012.pdf
[9] J. Pepitone, "Dropbox's password nightmare highlights cloud risks," June 2011.
[10] Cloud Computing, John W. Ritting House and James F Ramsome, CRC Press, 2012.
[11] Network Security William Stallings Pearson 2009

