ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Security Challenges and Solutions in Cloud Computing

Prof. D. G. Vyawahare[1], Rohit B. Bende[2], Dheeraj N. Bhajipale[3], Ravindra D. Bharsakle[4] , Amol G. Salve[5]

Assistant Professor and Head, Dept. of CSE, Anuradha Engineering College, Chikhli, Buldana , Maharashtra, India [1]

BE Student, Final Year, Dept. of CSE, Anuradha Engineering College, Chikhli, Buldana, Maharashtra, India [2,3,4,5]

ABSTRACT: Security strength defines the success of any network service ,with reference to last few years one of network driven service called cloud computing is very popular in IT sector because of it's various advantages.This survey paper aims to discuss, analyse security challenges and available solutions in cloud computing. To eliminate the security challenges in cloud computing we have explainedkey policy advanced encryption standard associated with user authorization period (KP-AESAP) allows user to decrypt data only within predefine authorization period.Ciphertext generated by AES is utilized by National Security Agency (NSA) of US for top secret information states high level security assurance[8].In proposed scheme ciphertext is coded with authorization period while private key is coded with a time instant so that ciphertext can only be decrypted by registered users havingkey with time instant between authorization period defined while encrypting file and substitution-permutation network associated with the ciphertext satisfy the key's access structure. The sensitive data will be securely self-destructed after expiration of user authorization period as ciphertext can't be decrypted beyond predefine time interval. (KP-AESAP) scheme proposed by us satisfies the security requirements and is better enhancement over existing schemes.

KEYWORDS : Advanced Encryption Algorithm , User Authorization Period ,Ciphertext , Sensitive data , security Challenges

I. INTRODUCTION

Cloud computing is the best platform for kind,omnipresent, on-demand network access to a set of resources like worldwide networks, end user's system,cloud servers, memorystorage, software products and servicesthat can be rapidly utilized for data exchange between client and cloud server. Now a days use of cloud storage is on it's peak value and plays significant role in people's life. Users of cloud storage are requested to upload their data to corresponding cloud service provider.Users expect security from cloud service provider but they are unaware about data leakage through multiple cross cloud networks, outsourcing, caching. Data exchanged by cloud serverswithin workgroup, friend circle often contains owner's sensitive information (e.g. industrial development plans, financial data, health records , personal profile, secret codes etc.) and needs to be well protected. Data communicated over cloud may be hackby unauthorised users to use data against owner or to harm the owner of data. Therefore some challenges regarding security of data stored on clouds exists. Self destructive clouds, secured clouds are applied to solve the security issues of cloud storage.

A. *Cloud computing classification :*

On the basis of services offered and deployment model cloud computing is categories into three groups and considered as three layers of cloud computing

1. Software as a service :

It is the uppermost layer offers specific application as a service on demand. Application is hosted by service provider and utilise by users without installation , maintenance of application

2. Platform as a service:

It is middle layer offers platform for execution of user's application.

3. Infrastructure as a service :

It is lowest layer offers infrastructure to share various computing resources among different users.

B. *Cloud services are also deploy according to user requirements as describe below :*

1. Private Cloud: Cloud infrastructure is utilised by restricted users and it is maintain by organization itself or from cloud service provider.
2. Public cloud : No access restrictions on users. On public cloud multiple organizations can carry out exchange of data.
3. Community cloud : Cloud infrastructure is shared by organizations for some relative purpose
4. Hybrid cloud : A combination of two or more cloud deployment models to carry of exchange of data is called hybrid cloud.
5. Mobile cloud : With the innovation of 3G, 4G ,WiMax networking technologies and smart mobile technology access to cloud servers through mobile for data exchange is possible and efficient so the mobile cloud is used[11].

To overcome security challenges in cloud storage we have proposed a key policy called (KP-AESAP) advanced encryption standard associated with user authorization period[1].

II. SECURITY CHALLENGES IN CLOUD COMPUTING

1. Administrative access: In case of cloud environment administrative access is done through network that enables high exposure and risk .
2. Data Transmission :In Cloud computing most of the data is not encrypted while processing that may be used by intruder for modification. Cryptographic attacks like man in middle are carried out when there is intruder between communication path which can interrupt or alter communication.
3. Virtual Machine Security :To execute number of process on limited physical servers virtualization technique is used in cloud computing. Because of dynamic nature of virtualization it is difficult to maintain security. Vulnerability was found in files shared mechanismof virtual machine that grants users of guest system that can read or write any host file , security file.
4. Network Security :Domain Name Server (DNS) attack , Sniffer Attack , Reuse of (Internet Protocol) IP network challenges are associated with network security . DNS is used to convert domain name into IP address but in DNS attack user is routed to other than original cloud. Connection between sender and receiver get rerouted through some intruder connection. Sniffer attacks are launched by applications and capture data packets flowing through network that are not encrypted. Reuse IP challenge also exist as old IP remains for some time lag into DNS cache which can be assign to new user that can alter the data .
5. Data Security : Data stored on cloud server is not encrypted by default, users must have to encrypt data before storing it on cloud therefore there are security challenges exists regarding data that resides in clouds.
6. Data Integrity : Loss of data can happen at any level in clouds. Each transaction of data follows ACID properties (Atomicity, Consistency, Isolation , Durability).
7. Data Privacy : As cloud computing involves exchange of data with users , other cloud servers there are chances of data leakage from cloud or unauthorised access to stored data. Now a day cloud servers might contains user's sensitive data so privacy is needed but not properly preserved.
8. Data Availability: Uptime is not 100 % of some cloud servers so user can't access data stored on cloud.
9. Cookie Poisoning: In application as a service cloud contents of cookie are alter to access webpages to hack user data. This security challenges are observed in in cloud computing [12].

III. RELATED WORK

Number of systems was proposed to overcome security challenges in cloud environment but they need to be enhanced to increase security level. In[2] author explains fundamental idea of self destruction to secure cloud storage called vanish method where a decryption key is isolated and divided into random number of shares and then stored in a point to point connected system with distributed hash tables to maximize security. Unique value which is coded while encrypting is used to regenerate decryption key which is spread in form of shares.Some distributed hash tables support timeout variable which are used to assign lifespan to shares of key.Because of the Cryptographic techniques coupled with global-scale,point to point method, the system can maintain secure keys as hash tables will refresh periodically. Security provided by vanish is applicable for E-mails and other digital documents where stored, copied, cached data will not last beyond defined span of utilization it get automatically destroyed without involvement of both users and third party.Shamir secret sharing Algorithm was proposed to secure cloud storage where key is divided into different parts and while decrypting data proper integration of all key components is required[3]. Related distributed algorithm associated with session keys is proposed in [4] where distributed key as well as ciphertext needs to obtained from distributed hash table.

A. *Research issues in cloud security are :*

1. Data Encryption : Encryption is the key policy used to protect data. It is better if cloud servers automatically encrypts data when user uploads data.
2. Access Mechanism : Strong authentication process must be used. To reset or alter authentication attributes like password secure method must use.
3. Digital Signature : Use of digital signature for exchange of data ensures security as only intended user can access data .[10]

IV. PROPOSED SCHEME

To enhance , increase security at higher level we proposekey policy advanced encryption standard associated with user authorization period(KP-AESAP). In (KP-AESAP) while uploading data or file on cloud it will encrypted using advanced encryption standard algorithm along with specific user authorization period. A list of authorised users that can access uploaded data is also maintain. This assigns lifespan to uploaded data means data stored on cloud is usable within lifespan beyond that data will not exist. To retrieve or download data which is on cloud user must have a instant primary key within specified user authorization period. In case user authorization period is expired and primary key is used to decrypt data that was uploaded on cloud will not be decrypted further and gets self destructed as it can’t be converted into plaintext[6]. For any user who want to utilize system required to get register on system with username and password which will used for security purpose. In proposed scheme advanced encryption standard(AES) algorithm is used to encrypt the data that is highly secured, larger key size is supported by (AES) upto 168 bits , faster execution in hardware as well as software , follows international standards of cryptography [9]

Algorithm to implement proposed scheme :

```
Step 1:Register on system with username and password.
Step 2: For uploading data or file
          Use AES(Advance Encryption Standard) with predefined user authorization period .
           Maintain list of users who authorised to access.
Step 3: Decryption key get limited valid instant
Step 4:For downloading
         While user = authorised
          If instant key <  predefined user authorization period
         Start downloading
         Else write : You are not authorised to download data or data can’t be download [6][7].
```

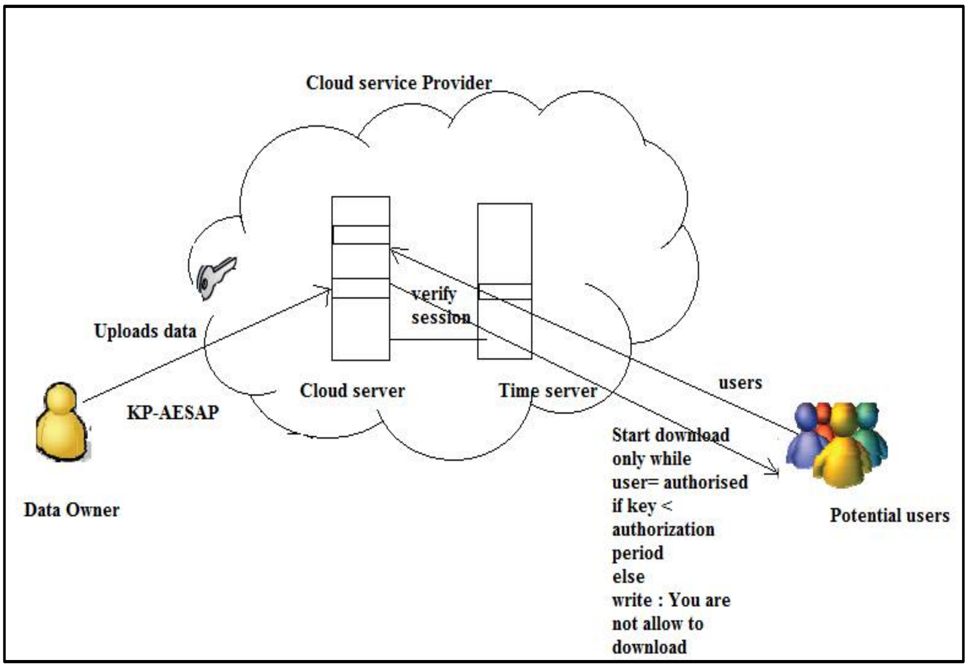
Given algorithm explains procedure to securely communicate data over cloud servers.

Modulesof proposed scheme :

1) Registration : To utilize services provided by proposed scheme owner or user of data require to get register on system to obtain username and password
2) Login: Users must login to access services.
3) Set of functions: In this module of system upload file , authorise users , download file , generate authorization period functions are implemented.
4) Directory: This Module consists of encryption / decryption programs, administrator’s tool .
5) Cloud server: connected to directory module to exchange data with users .
6) Time server: To verify session of data exchange over cloud server by users by checking valid decryption key having value specified in user authorization period along with authorised user[1].

DOI: 10.15680/IJIRCCE.2016. 0403086

V. ARCHITECTURE DIAGRAM



VI. CONCLUSION & FUTURE WORK

In this paper we have survey various security challenges and available solutions in cloud computing.One among various security challenges in cloud computing is worry about sensitive data which is communicated over cloud. We expect that security challenges, research issues analysed here provide good understanding that leads to future research.To enhance security in cloud computing we proposed primary key valid by time instant , uploading data with advanced encryption standard algorithm along with user authorization period . With application of propose system data residing on cloud can only access , downloaded when proper integration of various conditions are achieved . If conditions like a instant primary key within specified user authorization period by authorised user are not satisfied then uploaded data can't be access or downloaded . In case data leaks in adverse condition it remains in encrypted form and gets self destructed[1].We have propose this system for limited data types , file types that can be exchanged over clouds so there is scope for future work to implement same system for different file types , data types.

REFERENCES

[1] JinboXiong, *Student Member, IEEE,* Ximeng Liu, *Student Member, IEEE,* Zhiqiang Yao, Jianfeng Ma, Qi Li, KuiGeng, and Patrick S. Chen "A secure data self-destructing scheme in cloud computing" IEEE TRANSACTIONS ON CLOUD COMPUTING VOL:PP NO:99 YEAR 2014

[2] Roxana GeambasuTadayoshi Kohno Amit A. Levy Henry M. Levy, "Vanish: Increasing data privacy with self- destructing data," in Proc. USENIX Security Symp., Montreal, Canada, pp. 299–315, Aug. 2009.

[3]A. Shamir, ―How to share a secret, Communications of ACM, vol. 22, no. 11, pp. 612–613, November 1979.

[4]AnujaPalande, ChaitaliRao, PoojaRodi, VrundaBhusari "Self-Destructing Data System using Shamir secret sharing Algorithm" *(IJAIEM)* Volume 4, Issue 1, January 2015 ISSN 2319 – 4847 pp. 211-213

[5]N.S.Jeyakarthikka, S.Bhaggiaraj, A.Abuthaheer, " Self Destructing Data System Based On Session Keys" INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 2, FEBRUARY 2014 ISSN 2277-8616 340

[6] Lalitha K, Sasi Devi J "SEDAS: A Self Destruction for Protecting Data Privacy in Cloud Storage As A Service Model" International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 1, February 2014

[7] Shankar Gadhve, Prof.Deveshree Naidu "Self Destruction System for Protecting Data Privacy in Cloud Storage"IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015. Pp. 986-989

[8]FACT SHEET CNSS Policy No. 15, Fact Sheet No.1, June 2003

[9]https://www.quora.com/Cryptography

[10]Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez "An analysis of security issues for cloud computing" Hashizume et al. Journal of Internet Services and Applications 2013, 4:5

[11]RohitBhadauria, School of Electronics and Communications Engineering Vellore Institute of Technology, Vellore, India .SugataSanyal ,School of Technology and Computer Science Tata Institute of Fundamental Research, Mumbai, India "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques"

[12] Rabi Prasad Padhy , ManasRanjanPatra , Suresh Chandra Satapathy " Cloud Computing: Security Issues and Research Challenges" RACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011 pp. 136-146

BIOGRAPHY

Prof. D. G. Vyawahareis working as assistant professor and head of Computer Science and Engineering Department of (AEC) Anuradha Engineering College , Chikhli-444 201 (M.S.) since 2012. He has 8 years of experience as Assistant Professor and 9 years in industry .

Mr Rohit Bharat Bende , Mr Dheeraj N. Bhajipale , Mr Ravindra D. Bharsakle , Mr Amol D. Salve are Final year Students of Bachelor of Engineering in Computer Science and Engineering Department of Anuradha Engineering College Chikhli-444 201 (M.S.)

DOI: 10.15680/IJIRCCE.2016. 0403086