International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Secure Online Encryption and integrity checking with Partial Data Identity Outsourcing

Ms. Spoorthi.T [1], Mrs. Rekha M.S[2]

[1] *Dept. of Computer Science and Engineering, Impact college of Engineering & Applied Science, Sahakar Nagar, Bangalore, Karnataka.*

[2] *Assistant Professor, Dept. of Computer Science and Engineering, Impact college of Engineering & Applied Science, Sahakar Nagar, Bangalore, Karnataka.*

***Abstract*—*Day by day it is becoming necessary and feasible to use cloud storage due to its flexible and secure services. As more number of users are adopting cloud data services different types of threats are troubling them. In such scenario available Cloud Service Provider's security services may seem insufficient to keep user's data safe. User level security mechanism helps to improve security and user's trust in adopting the cloud data services. In our system we have implemented online data encryption mechanism. It is used at user level in which data to be uploaded to cloud storage is encrypted at the time of uploading. Online data encryption helps to fasten the process and saves user's time. To provide better data access control we have used a strong data security technique in which user's data identification credential and salt is used. Data identification credential, partial element of cipher key, is outsourced to cloud for further use in data decryption process. Decryption process is performed at the user level with the help of salt and one time password. In this system user is kept free from key storage and management task as well as it incorporates advanced and more secured technology of containers to store data in cloud. Researchers introduced Proof of Storage (PoS) [15] for checking the integrity without downloading files from the cloud server. Furthermore, users may also require several dynamic operations, such as modification, insertion, and deletion, to update their files, while maintaining the capability of PoS. This paper incorporates the detailed analysis of results obtained.*

Keywords **— cloud data security; salt; online encryption; use of containers; blob storage**

I. INTRODUCTION

Cloud computing is a relatively new business model in the computing world. According to the official National Institute of Standards and Technology (NIST) definition,

"Cloud computing is a model for enabling ubiquitous, 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".

Cloud model comes with five essential characteristics as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service. NIST defines three types of service models Infrastructure as a Service(IaaS), Platform as a Service(PaaS) and Software as a Service(SaaS) that cloud offers and four deployment models viz private, public, hybrid and community[1,2,3].

Fig.1 shows the NIST's high level cloud computing reference architectural view [3]. The architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing.

Table 1 briefly lists the actors defined in the NIST cloud computing reference architecture [3]. Here security is a subcomponent of the Cloud Provider.

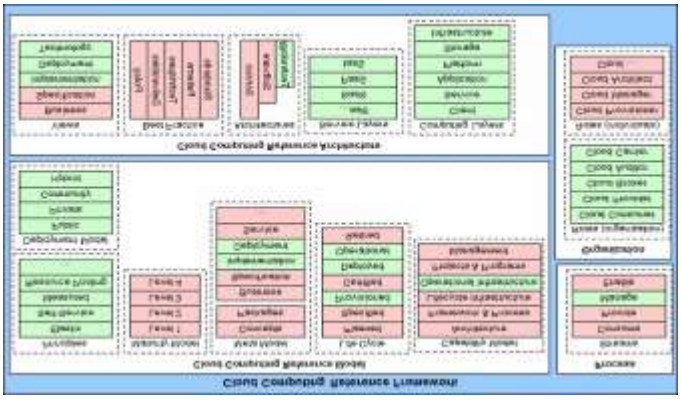

Figure 1. NIST cloud computing reference architecture Today use of cloud computing services has remarkably increased. Small scale industries to large scale are relying on cloud services to reach the end user. Even single users are switching from traditional storage to cloud storage due its economical secure services. Wide popularity of cloud services has increased risks for its users.

Gartner has defined seven popular threats about cloud computing environment [1,4]. But now the things have changed a lot. Users using cloud services have gradually increased which has caused new security threats, risks and challenges to be peeped out. Recently in January 2016 Cloud Security Alliance (CSA) has released the report "Treacherous 12" revealing top 12 cloud computing threats organizations face in 2016 [6]. As new problems are arriving on the way we need to come up with new solutions to solve them.

In addition with Cloud Service Provider's (CSP's) security services user should have his/er own security mechanism to sustain against vulnerable situations those occur in cloud environment time to time.

Fig 2: Actors in NIST cloud computing reference architecture

II.LITERATURE SURVEY

In cloud computing environment faces of security threats, challenges have been changing very rapidly. Many companies such as Amazon, Google, IBM, Microsoft have speed up the development of cloud computing systems and improving their services to provide trustworthy environment to users. However, security and privacy issues are strong obstacles for users to adopt cloud computing system with confidence as it is not capable to ensure strong security in terms of data privacy, integrity. Some of cloud services such as AWS, CipherCloud, CSA have been studied in addition with other literature.

Amazon Web Services (AWS) founded in 2006, provides a secure, scalable cloud computing platform with high availability, offering flexibility to develop a wide range of applications. AWS helps to protect the confidentiality, integrity, and identity of their customers' systems. Amazon Web Services Marketplace has various security solutions offered by hundreds of ISVs, spanning infrastructure security, logging and monitoring identity and access control, data protection and many more. AWS marketplace allows user to use any of the product on pay per as you go basis (hourly/monthly/yearly) and offers bring your own license (BYOL) options. AWS key management system(KMS) is a managed service that makes it easier to create and control the encryption keys used to encrypt data and uses hardware security modules (HSM) to protect security of keys. Vormetric Transparent Encryption for AWS secures cloud data at rest with on premises key management granular data access control. Gemalto'sSafeNet Protect V allows customers to retain as much control of encryption keys as possible. It secures sensitive and highly regulated data residing in Amazon EC2 instances and Amazon EBS volumes. SafeNet Protect V and SafeNet Virtual KeySecure allow user to own data and its encryption keys [10,11,14,20].

CipherCloud founded in 2010, provides enterprise cloud security offers in Security as a Service (SecaaS). It is a leader in cloud visibility and data protection, delivers cloud adoption while ensuring security, compliance and control. CipherCloud provides SecaaS for applications in Financial Services, HealthCare & Life Sciences, Technology & Supply chain, Government, Telecommunication, and Gaming etc. The CipherCloud Platform secures multiple cloud applications including Salesforce, Force.com, Chatter, Gmail, Office 365, and Amazon AWS. CipherCloud's framework lets users keep their data confidentially on public cloud frameworks. CipherCloud Encryption Gateway provides a way for companies to encrypt sensitive information in cloud email. As per the level of protection needed user can select encryption algorithm to be used for securing email. It comes with AES-256 as a strong encryption. Cloud gateway uses a FIPS 140-2 validated cryptographic module. Recognized by Gartner as a Cool Vendor in Cloud Security in 2011. CipherCloud is only provider of unified cloud data protection gateway. CipherCloud Encryption Gateway provides encryption to cloud email. It keeps key registry with the company in which user is working [9]. If key database is lost by company user is no longer able to access data [12,13].

The Cloud Security Alliance (CSA), founded in 2008. They are subject matter expertise of industry practitioners, associations and governments. CSA offers cloud security-specific research, education, certification, events and products to their corporate and individual members. CSA's comprehensive research program works in collaboration with industry, higher education and government on a global basis. SecaaS group within the CSA has been created to provide direction to deliver security services to cloud. CSA provides security at all cloud models- IaaS, PaaS, SaaS. Encryption (Cryptography) tools and key management service (KMS) are provided to secure the data against unauthorized access. Support for Identity-Based encryption techniques. Supports standard encryption algorithms such

as AES, Blowfish, and RSA etc. Digital signature techniques are used to maintain trust and integrity [5, 6, 21].

Multi-tier authentication is proposed in [15], where it has taken two-tier authentication scheme. This scheme provides better security and provides user privacy preservation. In this scheme data privacy protection is not considered.

Availability of data is a major concern. The scheme of data splitting and replicating at various locations is proposed in

[17]. This paper has proposed semi and fully anonymous attribute based privilege control scheme to address user privacy problem in cloud storage server.

Cloud computing adoption framework (CCAF) is discussed in [18]. This framework is multi-layered security containing three layers first firewall and access control, second identity management and intrusion prevention and third is convergent encryption. This framework has incorporated hardware as well as software aspects in its built. Location based encryption is introduced in [19]. In this system user's location is considered as key element to decrypt the file.

As per our knowledge we found that Cipher Cloud is the closet to our system. With Cipher Cloud Encryption Gateway keys are kept with the company or organization wherein in our system we are not keeping any keys with user. This approach makes our system free from key storage and management task and free from any risk of exploiting data authorization.

III.INTRODUCTION OF SYSTEM

User can upload data to cloud in one of the two ways.

- Offline encryption
- Online encryption

In the first method user selects files to be uploaded from his/er local storage and encrypts them. Then user activates the online services and uploads this encrypted data to cloud. In the second method user is capable of doing the process of encrypting and uploading data in parallel.

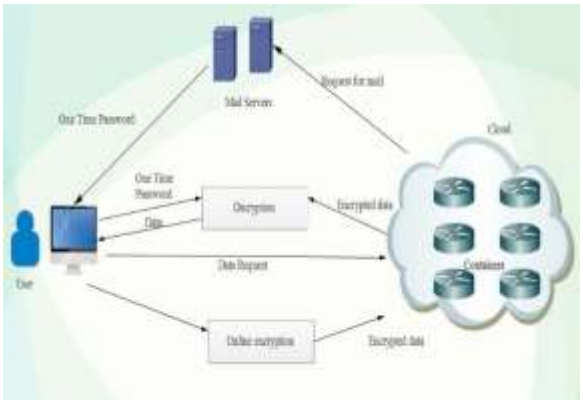

Figure. 2 General flow of the scheme

In the first method user unnecessarily gets involved in a lengthy process whereas the second method saves user's time. Our system has used the second method. Containers are used in our system to store data in cloud which makes it more secure.

At the time of data retrieval user has to login through his/er authenticated account. After successful login user selects the file to be downloaded. This file is in encrypted format. When CSP gets this request of data retrieval it sends One Time Password (OTP) on his/er authorized email-id. This OTP is used for data decryption process. Downloaded encrypted file is stored at user's site and decryption process is done at user's site itself. Only after entering correct OTP user is allowed to decrypt the file and see the contents of it. Hence OTP provides security to data.

A. Cloud Computing Security Threats

Minimizing the risk of adopting cloud data services means identifying the threats and providing solutions to them. Due to shared, on demand nature of cloud various security issues are raising and to withstand against them we need to have various suitable mechanisms. These mechanisms can be categorized at two levels based on its use

- Cloud service provider level
- User level

The security mechanisms used by CSPs are grouped under cloud service provider level and the security solutions used by individuals are considered at the user level. At user level individual may be a single user or a company or a part of community. The user level security mechanism is an additional effort to keep user's data secure. This mechanism is going to work as a security service in addition with CSP's security services. Our system is used at user level which provides protection shield for data in addition with CSP's security mechanism.

In this section we will focus on the security threats those we have considered in system.

- Data breaches: Cloud handles vast amount of data and its users. Hence it is very common that CSPs become target. Occurrence of data breaches is one of the threats which causes severe problem since it exposes user's financial, health and intellectual property data. Whenever data breaches occur companies do their procedure involving lawsuits and criminal charges. But ultimately data breaches take away the personal and sensitive information to the intruder also it affects the business of both client and service provider [6]. We may not be able to stop data breaches completely but we can have solution to keep user's data safe. Our system provides fourlayer security to user's data which helps to keep data safe even if data breaches occur in cloud environment.

- Compromised credentials and broken authentication: Single-tier authentication systems, weak passwords may result in data breaches. Key management system (KMS) is one of the critical taskin cloud computing as it contains very sensitive data related to users' credentials. Poor KMS gives open access to attackers. Multi-factor authentication is one of the solutions to this threat but sometimes this also doesn't seem perfect [6]. In our system key used for data encryption is not stored anywhere and hence this system is free from the risk of compromising credentials.

- Malicious insiders: Insider threat may be a contractor, business partner or any known person. That person may hack all information and hence the system depending solely on CSP services is at the high risk [6]. In the given system as no KMS is required so malicious insiders threat becomes ineffective.

B. Key Features of System

Our system has following key features-KMS free: As discussed in the previous section our system doesn't keep any record of keys or passwords used throughout the execution and hence key storage and management is not needed. This strengthens the system against insider attacks.
• Online data encryption: This idea saves user's time required for uploading data to the cloud. Normally user does the process of data uploading through two different tasks. In the first task user encrypts the data locally by using his/er own encryption method. In the second task he/she uploads this encrypted data to cloud through CSP. Our system uses online encryption which allows user to perform these two tasks as a single task. In this system user has to just select the file to be uploaded and provide the security credentials and rest of the process is done by the system. This process combines two different tasks together which reduces the execution time.

- Four layer security for data: Data in the cloud is kept in the shared environment due to which data access control and privacy preservation is one of the prime importance. In our system data is protected with four layer security mechanism depicted in fig.3.

- In built security mechanism of cloud data services (Microsoft Azure Emulator):This security layer incorporates in built security features of Microsoft Azure Emulator service.

- One Time Password (OTP):This layer permits authenticated user to decrypt the downloaded data by entering OTP received on his/er authorized mail-id. This OTP plays role of a partial element to generate the decryption key. This layer assures user about data authorization.

- Two layer encryption key generation: This layer has two sub layers to produce key used for data encryption. Details of key generation are discussed in the following section.

- Salt and UDIC: Use of these two parameters to generate encryption key makes system to withstand against dictionary attacks and rainbow attacks IV.

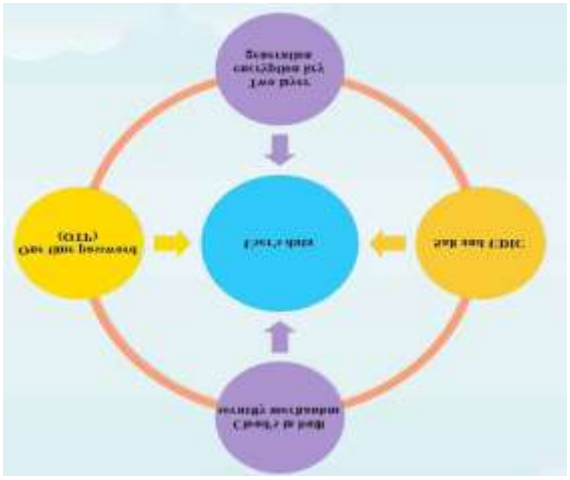

Figure 3. User's data security scenario

IV.PRELIMINARIES

Here we will see the terms those are related with our system.

A. Salt

It is the string which is prepended or appended with security token before hashing to randomize hash. Usually hashing is done for storing passwords of users. In traditional method password of user is hashed and stored in database. When user enters password for authentication its hash value is calculated and checked with the hash value retrieved from the database. This method is vulnerable to lookup table, dictionary, brute force, reverse lookup and rainbow table attacks. Adding salt makes lookup tables, reverse lookup tables and rainbow tables attack ineffective [7]. Here in the system salt is used in combination with UDIC token to protect ownership of data. Longer the size of salt difficult is to crack the data. In this system salt used is of 128bits.

B. User's data identification credential (UDIC)

To put data in the data owners hand safely is the prime aim of cloud data handling services. User authentication is used everywhere as the primary tool for authorization. There are mainly three authentication factors viz knowledge factor (username/password), possession factor (smartphone/OTP token) and identity factor (fingerprint etc.) [15,16]. Conventional authentication technique using username/ password is insufficient since it is prone to insider attacks. On compromising password results in losing whole thing. In such scenario system should provide the way to keep data safe even if personal credentials have been compromised and here UDIC comes in picture. In given system user is asked to provide UDIC token which is used to encrypt file/data. Data owner is allowed to enter any size of UDIC token. This token along with salt is used to generate encryption key for data. Importantly no key is required to store at any place for future use. Details of key generation are discussed in the following section.

C. Containers

Small pieces of software called micro services are now a days used to perform specific task. They are loosely coupled hence can be changed at any time. These services needed to be transported across various environments and infrastructures. To fulfill this need Docker introduced containers in 2013 which in turn emerged as Containers as a Service(CaaS). It provides agility, portability and control for developers and IT operations team. CaaS provides a framework which considers needs of developers and operations and provides various capabilities and consistent Application Program Interface (API) across entire platform for ease of team to team transition. Docker also supports all stages of life cycle during application development irrespective of infrastructure environment, tools, languages and operating system used to build it. Docker comes with open platform which provides more flexibility to IT developers. Containers although are flexible provide security in cloud environment. This attracts cloud user for deploying application modules or any other services [8].

D. Microsoft Azure Emulator

Microsoft Azure Emulator provides a local environment that emulates the Azure Blob, Queue, Table services for development purposes. In the given system Blob storage also known as Object storage is used which is useful for storing unstructured object data such as documents, photos, videos, music blogs, backup of files etc. Every blob is organized into a container and a container can have any number of blobs. Blob size supported by storage emulator is upto 2GB. It supports block blob and page blob operations [9]

E. Dynamic Proof of Storage

Dynamic Proof of Storage (PoS)[16] is a useful cryptographic primitive that enables a user to check the integrity of outsourced files and to efficiently update the files in a cloud server. Although researchers have proposed many dynamic PoS schemes in single user environments, the problem in multi-user environments has not been investigated sufficiently.

V.SYTEM DETAILS

Data storage is one of the widely used popular services provided by cloud computing. This service with plenty number of advantages comes with darkness of security and privacy issues. Even though CSPs ensure customers for safety of their data, customers hesitate to rely on them and step back from adopting data services of cloud. Customer's hesitation comes due to various threats of cloud environment [5,6,10]. Our system tries to resolve the threats such as data breaches, compromised credentials and broken authentication, malicious insiders and provides investigate support. System performs various functions viz authenticating user, generating private key for encryption, online encryption, auditing data. Authentication is a primary and essential element of typical security model. Log on authentication mechanism using knowledge factor is used here in which user has to enter login id and password. After successful login user is allowed to perform various operations on data such as uploading of data, downloading data and performing audit of it. User can have various types of data files such as documents, log record, music files, video files, big data files etc. This type of collection of data is called unstructured data. In the system we have used containers to store data in cloud. As discussed in the previous section containers come with built in security mechanisms which provide additional security to data in cloud [8]. The system uses Azure Storage Emulator this allows user to upload data

size of up to 2GB [9]. After successful login authorized user selects the data files and enters two more parameters- UDIC token and salt.

There is no such restriction kept on the size of these two parameters. User can enter any size of UDIC token and salt. UDIC token is used as data ownership authentication parameter which prevents losing personal and sensitive information when user's personal credentials have been compromised. These two parameters are used to generate encryption key. Encryption process incorporates two layer key generation process depicted in fig. 4.

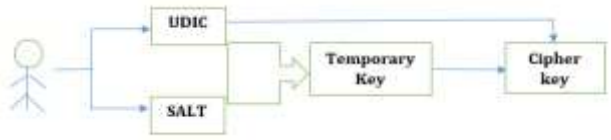

Figure 4. Two layer key generation for data encryption

The key generated in the first layer is used as input for second layer and processed resultant key is used for encryption. In the first layer salt and UDIC token is taken and processed to compute temporary key, Tkey, which is used in second layer for generating encryption key. In the second layer Tkey with UDIC produces encryption key .Due to this two layer key generation process done with the help of salt and UDIC makes our system a good choice to have better data access control. Algorithm 1 gives brief idea about generation of encryption key.

Algorithm 1: Algorithm to generate encryption key

Inputs:

Uudic = User's data identification credential from user of n bits size

Usalt = Salt given by user of n bits size

Tkey = 128 bit key generated after first pass

Ekey = 128 bit key resulted after second pass

Compute:

U udic ← ConvertTo128bits(Uudic)

U salt ← ConvertTo128bits(Usalt)

T key ← ComputeTempKey(Usalt,Uudic)

E key ← ComputeExpandedKey(Tkey, Uudic)

Throughout this process no key is stored. Generated key gets utilized and destroyed immediately. The UDIC entered by user is stored with cloud service provider to be used during data decryption process as a OTP.

Algorithm 2: Algorithm for data encryption

Inputs and terms:

D = { D0, D1, D3,……..,Dn}

Ekey = Expanded encryption key

Db= Byte array representation of data

De = Encrypted byte array

Compute: for eachDn Є D do

Db← memstreamTobytearray(Dn)

De ← Rijndael(Db, Ekey)

Container ← De

end for

Successfully generated encryption key, Ekey, is passed to encryption module. Rijndael algorithm is used for encryption. In the system encryption is done at the time of uploading data. Rijndael is a block cipher algorithm chosen by NIST as the Advanced Encryption Standard (AES) in 1997. Rijndael works in parallel over the whole input block. It requires less memory. It can stand against power, timing attacks and brute force attacks. Though it comes with such attractive package it is simple in design and hence efficient in implementing both hardware and software. It comes in key size variations of 128 bits, 192 bits and 256 bits. In the system 128 bits key is used. With 128 bit key size there are 2128 = 3.4 X 1038 possible keys. A personal computer that tries 255 keys per second needs 149 billion years to break the key [22, 23]. In the system breaking of key is made even harder by adding 'salt' flavor. Algorithm 2 depicts idea of encryption process. There are D0, D1, D3,……..,Dn data blocks.Ekey is the outcome of key generation module of the system.

These techniques are not suitable for cloud storage services where users may check the integrity frequently, such as every hour[14]. Thus, researchers introduced Proof of Storage (PoS)[15] for checking the integrity without downloading files from the cloud server. Furthermore, users may also require several dynamic operations, such as modification, insertion, and deletion, to update their files, while maintaining the capability of PoS[15].

Algorithm 3: Algorithm for data decryption

Inputs and terms:

D = { D0, D1, D3,……..,Dn}

UOTP = OTP received via OOB

Db= Byte array representation of data

Rkey = Key generated using OTP

Compute:

Rkey←KeyGeneration(UOTP)

for eachDn ϵ D do

De←Decrypt(Dn,Rkey)

Dm ←bytearrayTomemstream(De)

Restore decrypted data in file on local storage

end for

At the time of downloading user selects the file to be downloaded. On receiving download request system sends one time password (OTP) through out of band (OOB) mechanism on his/her authorized email-id. If user fails to enter correct OTP he/she is not able to decrypt the file. Algorithm 3 gives brief idea about decryption process.

VI.EXPERIMENTAL RESULTS AND ANALYSIS

We have used Microsoft Azure Emulator which gives local environment as of the Azure Storage services. This gives a testing platform for developer to test the application. Given solution can withstand against the threats those are listed in table 2. Using Proof of Storage algorithm we have checked the integrity without downloading the files. Further work, we can update the file such as modifications, insertions, deletion, etc.

Security Threat	Details	Solution in our system
Data Breaches	Whenever it occurs personal sensitive information goes in wrong hands	Our system provides four layer data security which ensures user about his/er data privacy in case of data breaches
Compromised credentials and broken authentication	This occurs due to weak passwords and traditional password processing techniques	Our system has used 128bit key for data encryption which is generated in two layers. Use of salt with UDIC token provides strong data authentication
Malicious Insiders	Any known person gets the credentials and can perform malicious activities	Our system doesn't keep any registry for data encryption keys and hence user's data is kept secure from malicious insider attacks

Results for the system have been checked on –
Pentium® Dual Core of 2.30GHz,

2GB RAM,

500GB HDD. The methodology used for system is - Windows 10 with Tomcat server, Microsoft Azure Emulator 2.0, Eclipse IDE, Google chrome.

To take the results we have implemented two different systems one using offline encryption process and second using online encryption process. In both systems only the way of encryption process and decryption process has been changed rest of the things such as algorithm used for encryption and key generation process are all same.

VII. CONCLUSION

The idea of online encryption process has saved user's time. The four layer security mechanism provided for data improves data access control and data privacy protection which are one of key challenges in the cloud environment. The security scheme using UDIC token and salt provides data privacy and keeps data safe even when data breaches occur.

Moreover system is free from key storage and management and uses containers for data storage in cloud which makes this system more secure. We can check the integrity of the files without downloading using Proof of Storage. User's data identification credentials one out of two cipher key elements we are outsourcing, in case even if it gets hacked it will not be of any use since decryption key has to be generated with two elements.

This partial key outsourcing makes user's data ownership more transparent and increases trust of user in cloud data services.

REFERENCES

1. Rajani S. Sajjan, Dr. Vijay R. Ghorpade, "Secure Online Encryption with Partial Data Identity Outsourcing: An Exemplar for Cloud Computing", 978-1-5090-4884-7/17/$31.00 ©2017 IEEE.

2. Rajani S. Sajjan, Vijay R. Ghorpade,"Inside cloud computing: Exploring threats and risks", second International conference on current trends and challenges in management, engineering, computer application and technology, ICCTCMECAT-2012.

3. NIST definition of cloud computing, NIST Special Publication 800-145, http://csrc.nist.gov/publications/nistpubs/800145/SP800-

4. NIST cloud computing reference architecture, Special Publication, 500-292, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=90950

5. http://www.infoworld.com/d/security-central/gartner-sevencloud-computing-security - risks-853.

6. Cloud Security Alliance, "Top threats to cloud computing V1.0", March 2010 [6]. Cloud Security Alliance, "The treacherous 12 cloud computing top threats in2016"February2016.

7. Searchsecurity.techtargt.com/definition/salt

8. Docker, "Modern application architcture for the enterprise", January 21, 2016.

9. "Introduction to Microsoft Azure Storage", http://azure.microsoft.com/enin/documentation/articles/storageintroduction

10. Ashish Singh, KakaliChatterji,"A secure multi-tier authentication scheme in cloud computing environment", International Conference on Circuit, Power and Computing Technologies(ICCPCT) IEEE 2015.

11. Victor Cahng, MuthuRamachandran, "Towards achieving data security with the cloud computing adoption framework", IEEE Transactions On Services Computing, Vol. 9 No. 1, January/February 2016.

12. Meer SoheilAbolghasemi, Mahdi MokarramiSefidab, "Location based encryption to improve the security of data access in cloud computing", IEEE Transaction On Cyber Security, Vol 10, No.6, April 2016.

13. Kun He, Jing Chen, Ruiying Du, Qianhong Wu, Guoliang Xue, and Xiang Zhang," DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments", IEEE Transactions on Computers (Volume: PP , Issue: 99).

14. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. of SecureComm, pp. 1–10, 2008.

15. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. of ASIACRYPT, pp. 319–333, 2009.

16. C. Erway, A. K ¨upc ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS, pp. 213–222, 2009.

17. Mazhar Ali, KashifBilal,"DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE Transactions on Cloud Computing, TCC.2015.2400460.

18. Victor Cahng, MuthuRamachandran, "Towards achieving data security with the cloud computing adoption framework", IEEE Transactions On Services Computing, Vol. 9 No. 1, January/February 2016.

19. Ken Beer and Ryan Holland," Amazon Web Services: Securing data at rest with encryption", http://aws.amazon.com/whitepapers.

20. Meer SoheilAbolghasemi, Mahdi MokarramiSefidab, "Location based encryption to improve the security of data access in cloud computing", IEEE Transaction On Cyber Security, Vol 10, No.6, April 2016.

21. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing", V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pd f.

22. Joan Daeman, Vincent Rijmen,"The design of Rijndael AESThe Advanced Encryption Standard", November 26, 2001, Springer-Verlag

23. Harris Nover, "Algebraic cryptanalysis of AES: An overview.