

AN ANALYSIS OF CLOUD DATA SECURITY ISSUES AND MECHANISMS

Gowthami Garikapati¹, Yakobu D², GnaneswaraRao Nitta³, Amudhavel J⁴¹Department of CSE, VFSTR University, Andhra Pradesh, India¹gowthami.mokshith@gmail.com^{2,3,4}Department of CSE, KL University, Andhra Pradesh, India²yakobdsp83@gmail.com³gnani.nitta@gmail.com⁴amudhavel@kluniversity.in

Abstract: Cloud computing is an emerging technology in IT industry now a days. Cloud is a place where one can access the computational resources through online and billing process is on pay-per-use basis, reducing the infrastructure as well as management cost. Cloud users can access all the resources with no upfront investments which help to manage their applications. Cloud computing has got the primary features like pay-as-you-go, scalability, flexibility and elasticity. Apart from these beneficial features it has come up with a considerable issue called security threats. As there are many number of users, it is necessary to provision the resources to legitimate users securely. The main security threats in cloud are provisioning of information security, network security. Information security is providing security to the data in cloud where data may either owned by the cloud service provider or the consumer. Although there are approaches proposed by cloud researchers that were implemented using the cryptographic algorithms for information security, they are inadequate while addressing the issues like attacks, confidentiality, processing overheads etc. This paper contributes to provide concerns of data that is placed in cloud and various mechanisms to secure such data. It concludes by suggesting combination of RSA and Blow-Fish cryptographic algorithms to secure data as both of them has got advanced features to secure data in cloud environment.

Keywords: Cloud Computing, Data Security, Encryption Algorithms

1. Introduction

Cloud computing is a fast growing and emerging technology in the IT industry in recent

years. Not only the IT industry but also every organization is looking forward to adopt this technology. Cloud computing[1] enables the cloud users to access various computing resources like networks, CPU, servers, infrastructure, applications etc. through online with minimal effort. It is cost effective in which cloud service consumer will pay for what has been utilized by him. It is more beneficial for smaller enterprises as well as the individuals to develop the applications because it provides required resources without any initial payment. This technology mainly works with three modules. One is cloud service provider[2], who places the data or resources into the cloud. Second module is cloud service consumer who accesses the required resources from cloud. And the third module is a web interface through which cloud user can place the resources in the cloud or access the services of the cloud. These services are provided in terms of Infrastructure as a service, Software as a service, Platform as a service[3], Communication as a service, Network as a service and Database as a service etc. In simple words we can say that cloud computing provides its services on everything as a service basis. These cloud services can be deployed in any one of three cloud deployment models such as public cloud, private cloud and hybrid cloud[4]. Public cloud makes cloud services available to all users via internet. Privatecloud makes services available only to authorized party, and hybrid cloud has been made out of combining any of the two clouds (public, private, internal or external).

The growth of this technology is just because of its features. Key features of cloud computing are pay-as-you go[5], flexibility, auto scaling[6],

elasticity [7], self-service provisioning etc. According to pay-as-you-go, the billing process is done based on the amount of utilization of the resources. This feature is playing vital role for the rise of this technology. In spite of having such greater features, it come up with various disadvantages like possible downtimes, inflexibility, no hardware, lack of support and security issues[8]. The security issues are related to information security [9], network security [10], confidentiality, attacks etc. Providing security to data in the cloud from being accessed by illegitimate users is known as information security or data security which is subject of this paper. Also, information should be kept confidential according to the requirements of the cloud user. Because of such problems in security, this technology is far away from banking field. Data/Information security issues can be avoided by implementing various mechanisms like cryptographic [11] algorithms, Digital signature, single sign-on, public key infrastructure, identity and access management etc. Unfortunately, these existing approaches developed by cloud practitioners are found to be inadequate. Although they are implemented using above mentioned approaches, they are pruned to attacks like man-in-the middle etc.



Figure.1 Cloud overview

This paper contributes to provide concerns of data that is placed in cloud and various mechanisms to secure such data. It concludes by suggesting combination of IDEA and Blow-Fish cryptographic algorithms to secure data as both of them has got advanced features to secure data in cloud environment. When we compared with other cryptographic algorithms we hope that combination of these two algorithms may provide results better than other approaches.

Section - II describes the security issues related to data and related work carried out by various

researchers is given in Section-III, Section-IV explains the various security mechanisms proposed in literature to secure data with explicit focus on analyzing the merits and demerits of cryptographic algorithms which is followed by Conclusion.

2. Data Security

Cloud data is a collection of information or files regarding a individual person or an enterprise that is being stored in cloud. Cloud data usually suffers threats from various threat agents.

Anonymous Attacker: Is usually a non-trusted cloud service consumer without permission in the cloud.

Malicious service Agent: who actually intercept and forward the network traffic that flow with in a cloud.

Trusted Attacker: A trusted attacker shares IT resources in the same cloud environment as the cloud consumer.

Malicious insider: Who actually acts on behalf of cloud provider.

Hence Cloud data security has become the primary focus of cloud researchers.

Data security: Data security is applied as one of the privacy measure to protect the digitalized information to protect the unauthorized access to computers associated with databases and many websites. It also protects the data from corruption as many of the organizations needs to be more prioritized by size and genre. More than encryption, Data security mainly involves three service models in this cloud computing. Normally, data is having two states of threats in cloud security called as Data at rest and Data in Transit.

Data at Rest refers to the storage of data in clouds and Data in Transit refers to the movement of data in or out from the cloud. Based on the nature of data protection, confidentiality and integrity are the two mechanisms that are needed to protect the data.

Data at Rest: This state refers to the any of the data that can be accessed using internet and can be stored in the clouds. This is the technique that can acts as a backup as well as live data. In the earlier studies, it is difficult to protect the data at rest in many organizations if there is no private cloud. At this case, they do not have data in control. This becomes main challenge and can be resolved by a well maintained private cloud which is controlled carefully.

Data in Transit: This normally refers to the movement of data in the cloud. The data can be in the form of a database or a file that is stored in the cloud. This data can be requested at anytime, anywhere for future use at any location. Whenever

the data is uploaded to the cloud at any particular instant of time, it refers to the data in transit. This is a sensitive data that can be encrypted at any time like usernames and passwords. The unencrypted data also refers to the data in transit.

2.1 Security related issues of cloud data:

Data breaches: It is one of the regions in the cloud which gives the known data about all the users. And tends to huge effect on security [1].

Data loss/leakage: Due to insufficient authentication, authorization and audit controls, there are many ways to compromise the data such as deletion or alteration of records without backing up the original content. This would become a serious problem in the area of cloud computing [2].

Insecure Application Programming Interfaces(API's): These API's provides an internal and integral security to the cloud services based on their availability. These type of interfaces should be designed in a way to provide a better protection against both intruders and accidental attempts [2].

Malicious insiders: They are the intruders who reveal the employee's access to physical and virtual assets based on the employee monitoring and how they are analyzed. In the area of cloud computing, every organization needs not to be known the requirements of the technical details of the services that are delivered. The risks are high at this type of situations [2].

Unknown Risk profile: data about who shares your infrastructure may be related [2].

Cloud abuse: Service abuse means that attackers may abuse the cloud service and acquire the extra data available or destroy the interest of other users[9].

Shared technology issues: (IaaS) it is mainly based on shared infrastructure (e.g., GPUs, CPU caches, disk partitions etc.), but not designed for strong isolation properties for multitenantarchitecture [2].

Physical security: No idea about where the resources are running [3].

Data seizure Risk: Company has violated the law (risk of data seizure by (foreign) government)[3].

Data control: Who controls the encryption/decryption keys?[3].

Data integrity: Ensuring the data integrity which means storage, retrieval and transfer. Really means that it modifies only in response to legal transactions [3].

Data authorization: In Payment Card Industry Data Security Standard (PCI DSS) data logs should be provided the security managers and regulators [3].

Data availability: The aim for availability of Cloud Computing systems is to protect its users can utilize them at any time [8].

Data Access Control: the confidential data is hacked illegally due to lack of security [7].

Data location: When the user makes use of cloud computing services, don't realize this issue that data is stored in which place, and the service is located in what place?[5].

Data Confidentiality: Confidentiality means storing user's information securely in Cloud systems [8].

Data Relocation: Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another [4].

Recovery: the client doesn't know where the data is coming from, a cloud user will give the information to the customer. That leads to happening of data damage and does the user gives the restoration and so it takes much time to complete the task [1].

Investigative Support: the vendor ensures the capacity to scan any illegal activity [1].

Long-term possibility: ideally the cloud user neither get gained nor become poor [1].

Denial of service: Denial of a service consists of variety of techniques designed to deny users or client access to specific system and network resources. In denial of service attacks of resources are input-output, Network bandwidths, CPU utilization, Disk space and Memory utilization. Most common example of denial of service attack is the distributed DoS (DDoS)[6]

External attack: Scanning, Malicious cracking, and probing to gather infrastructure data. The examples are insertion of malicious code or virus [6].

Theft: The Physical theft of software or hardware, to steal the secret data for benefit is example [6].

Fraud: Collusion, data manipulation, falsified transaction, and other change of data integrity i.e. modification of information are the examples of fraud [6].

3. Related Works

Evaluating The Performance of Symmetric Encryption Algorithms presented by DiaaSalamaAbd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2. This paper presents a performance estimation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. Several points are concluded from the Experimental results. According to some different metrics as compared to these algorithms finally blow fish algorithms give the best performance of all metrics.

A novel triple encryption scheme for hadoop-based cloud data security present by chao yang, weiwei LIN, mingqi LIU. In this paper triple encryption scheme used for providing security for hadoop files. In proposed system HDFS files are encrypted by using the hybrid encryption based on DES and RSA, and the user's private key is encrypted by using IDEA. Finally get the result of experiment show the triple encryption scheme they proposed is feasible, it meets the reading and writing characteristics of HDFS and can enhance the confidentiality of default HDFS.

Secure file storage in cloud computing using hybrid cryptography algorithm present by punamV.Maitri and Aruna Verma.in this paper they have to introduced new security mechanism using symmetric key cryptography algorithm and steganography. AES, RC2, BRA, blowfish algorithms are used in proposed system to provide

block wise security data.LSB steganography technique is introduced for key information security. And multi-threading technique is also used for simultaneously encrypted of files. With the help of proposed security mechanism data integrity, high security, low delay authentication and confidentiality parameters are accomplished. Using proposed text file encryption need 17% to 20% less time as compare to AES algorithm. for AES text decryption needs 15% to 17% maximum time as compare to proposed system. In blowfish for encryption need 12% to 15% maximum time as compare to proposed hybrid algorithm text file decryption using hybrid algorithm need 10% to 12% less time with respect blowfish algorithm.

Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques", Vinay Kumar pant, JyotiPrakash This paper describes how to secure data and information in cloud environment in time of data sharing or storing by using our proposed cryptography and steganography technique. In tis they are using two algorithms cryptography by RSA. Steganography by RSA.RSA algorithm is more secure than other algorithm. We integrate RSA algorithm with other algorithm to provide more security to data. In steganography process we get encrypted image, which looks exactly the same to original image by human eye. If we analysis the image binary codes then the differences would be seen. Otherwise we are unable to identify the original image.

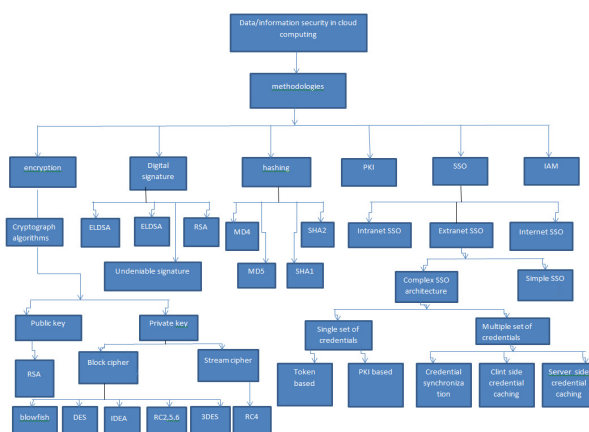


Figure.2 Data Security Mechanisms

This paper aimed to analyze the performance of various encryption algorithms basing on following parameters:

- i. Encryption/Decryption time.
- ii. Chi-Square Value
- iii. Buffer size
- iv. Memory size
- v. Avalanche effect
- vi. Entropy
- vii. Robustness against statistical attacks

viii. Invisibility

3.1 Comparing AES, 3DES, DES, RC2, RC6 and BLOWFISH with respect to their advantages and disadvantages:

Advantages:

AES: AES is more safety (it is less adaptable to cryptanalysis than 3DES). As compared to 3DES's AES supports large size of key. AES is speedy in both software and hardware. AES is not only satisfy security but also increase the performance in variety of setting like hardware implementations, smartcards etc. it is a federal information processing standard which are currently doesn't know non-brute-force attacks against AES. It is strong to be certified by the use of US government for top secret data.

DES: DES is avalanche effect which means if any change in key or plain text then there is a similar change in cypher text. This algorithm includes S boxes. It will be confuse the attacks to decrypt the message. Through RSA we get more secure cypher text between it is 70 times much better than symmetric key algorithm.

3DES: 3DES is a scheme to reuse the implementations of DES, by combining the three cases of DES (with distinct keys). It believed the security at least " 2^{112} ". But 3DES is slow mainly in software.

RSA: it is very fast, very simple for encryption and verification. It is easier to implement than elliptical curve cryptography algorithm [ECC]. It is widely deployed, better industry support. The number of keys are only twice of the number of user. One more advantage is individuals can post their public key on their website. it provide for message authentication and non-repudiation.

Blowfish: Algorithms available and the speed of the algorithms and key strength is also very good. Blowfish is a block cipher which is proposed by bruce Schneier. And it is deployed in some other software's. Blowfish can use large number of keys and it believes security, except with regards to block size. This means 64 bits like 3DES and DES. Blowfish is efficiently works in software, one on some software platforms. More secure than DES.

4. Conclusion

In this paper, we have provided concerns of data that is placed in cloud and various mechanisms to secure such data. It concludes by suggesting combination of RSA and Blow-Fish cryptographic algorithms to secure data as both of them has got

RC6: it is same as RC5 structure, using modular addition, data-dependent rotations, and XOR operations; RC6 could be seen as interweaving two parallel RC5 encryption processes. RC6 use an extra multiplication operation which is not present in RC5 in order to make a rotation dependent on each bit in a word, and not just the least important few bits.

RC2: RC2 uses a volatile key size, but it has 128 bit key would considered normally as good. RC2 is used in all modes but DES is used in a property algorithm which is developed by RSA data security, this algorithm enlarges a message up to 8 bytes. It is a block cipher which encrypts the data into blocks of 64 bits.

Disadvantages:

AES: the main challenge is to exchange that key with complete privacy as if this key is found then all the encryption process is useless. If loss of private key means that all received message cannot be decrypted. it take more time and need more processing. it requires more rounds of communication as compared to DES.

DES: brute force attack is possible by DES. If attacker perform 2^{55} combinations of plaintext and key automatically it reveal plaintext. DES fails in front of linear crypt-analysis because during its design this was not invented.

RSA: it takes more time for encryption and decryption. It is very slow process. If loss of private key means that all received message cannot be decrypted. as compare to 3DES and AES it is very less secure algorithm.

Blowfish: It needs to acquire a key to the user out of band currently not through unsecured channel. Each pair of users has to be different, so that the user's number increase, management of key becomes a issue. Blowfish can't allow authentication and non-repudiation as two users having similar key. It is also a disadvantage/lacking factor on process of decryption in compare to other algorithms with regard throughput and time consumption.

3DES: practically 3DES is not useful to encrypt large messages. And there is a difficulty of unsafe key transmission between the vendors. 3DES working process is very slow when compared to modern algorithms like blowfish and RC6.

advanced features to secure data in cloud environment. When we compared with other cryptographic algorithms we hope that combination of these two algorithms may provide results better than other approaches.

References

- [1] JagpreetKumar,SunnySingh,AmitKarn,"Analysi s of security issues and management standards in cloud computing",2015 IEEE.
- [2] Nedal, A. AL-Saiyd, Nada Sail, "Data Integrity In Cloud Computing Security"Journal of Theoretical and Applied Information Technology
- [3] KrešimirPopović, ŽeljkoHocenski , " Cloud computing security issues and challenges,
- [4] Puneet Kumar and Harwant Singh Arri, Data Location in Cloud Computing ,International Journal for Science and Emerging Technologies with Latest Trends” 5 February 2013.
- [5] S.MahadiShariati,Abouzarjomehri,M. HosseinAhmadzadegan, "Challenges and security issues in cloud computing from two perspectives:Data security and privacy protection",KBEI-2015.
- [6] PatilMadhubalaR,"Survey on Security Concerns in Cloud Computing", IEEE-2015.
- S.Rajeswari, M.S .Sushmitha, “Augmented Reality And Its Application”, International Innovative Research Journal of Engineering and Technology, 2016.
- [7] RandeepKaur,JagroopKaur"Cloud Computing Security Issues and its Solution:
- [8] BhushanA.Ugale, PiyushSoni, TseringPema, and AnirudhaPatil," Role of Cloud Computing for Smart Grid of India and its Cyber Security", IEEE-2011.
- [9] Dr. K.B.Priya Iyer1, Manisha R2, Subhashree R3,Vedhavalli K4,"Analysis Of Data Security In Cloud Computing",*International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16)*.

