Comparative Study of Cloud Computing Data Security Methods

Megna Unnikrishnan
P.G Student,Computer Science
Thejus Engineering College
Thrissur,India

Lipi Arun
Computer Science Department
Thejus Engineering College
Thrissur,India

ABSTRACT
Cloud computing is the concept implemented to decipher the Daily Computing Problems. Cloud computing is basically virtual pool of resources and it provides these resources to users via internet. Cloud computing is the internet based development and used in computer technology. The prevalent problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. The work plan here is to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud. Have discussed about cloud computing security mechanisms and presented the comparative study of several algorithms.

General Terms
Security, IaaS, PaaS, SaaS

Keywords
Cloud Computing, Algorithms :AES,DES,RSA

1. INTRODUCTION
Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Cloud computing is a model for allocating compute and storage resources on demand. The basic concept of cloud computing is to provide a platform for sharing of resources which include software and infrastructure with the help of virtualixation.in order to provide quality of service, this environment make effort to be dynamic and reliable. As in most other streams of computer, security is a major obstacle for cloud computing.

Data security is a very important aspect of quality assurance. At the outset, security must be imposed on data to gain the secured data location and access. Since the cloud is having open characteristics, it is having security problems. The cloud system is more powerful than personal computing but the data from wide angels such as internal, external threats for data located on the cloud. Since the data are not located into users area, establishment of security features cannot be implemented directly.

The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) all of which means a service oriented architecture. Here comes the first benefit of the Cloud Computing i.e. it reduces the cost of hardware that could have been used at user end. As there is no need to store data at user's end because it is already at some other location. So instead of buy in save bulk of data which you are just renting the assets according to your requirements.

SaaS deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, but also increases security risk. With this service model it's essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.

PaaS is a shared development environment, where the consumer controls deployed applications. Cloud infrastructure is not managed properly.Eg: Microsoft Windows Azure. This model requires an audit trail, strong authentication and the ability to support compliance regulations and privacy mandates.

IaaS lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared responsibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.

2. SECURITY ISSUES AND CHALLENGES OF CLOUD COMPUTING
Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Cloud Computing has several major issues and concerns, such as data security, trust, expectations, regulations, and performances issues.

There are several of security concerns connected with cloud computing but these concerns fall in to two broad categories: Security issues connected with cloud providers and security issues faced by their customers. In most of all cases, the organization must ensure that the services provided by them is secure and their clients data are protected and customer should have an assurance that the service provider has taken the proper security measures to protect their information in a significant manner.

Though cloud offers sophisticated storage and access environment, it is not hundred percent reliable; the challenge exists in ensuring the authorized access. The third parties make such a decision about our data, and therefore security remains as a big concern. So cloud applications must ensure that data accessed is by authorized users. Authentication and

identity management can help the users to authenticate and getting services based on their credentials.

2.1 Cloud Deployment Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has three main deployment models which are:

2.1.1 Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise data center[9].In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds:(i) on-premise private clouds and (ii) externally hosted private clouds.

2.1.2 Public cloud

The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off premises).All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization [10]. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

2.1.3 Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [11]. Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. It provides virtual IT solutions through a mix of both public and private clouds.

2.2 Challenges of Cloud Computing

One issue with cloud computing is that the management of the data which might not be fully trustworthy; the risk of malicious insiders in the cloud and the failure of cloud services have received a strong attention by companies.

2.2.1 Privacy and confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. In appropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential [1].

2.2.2 Data integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

2.2.3 Data availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

2.1.4 Identification and authentication

The multi tenancy in cloud computing allows a single instance of the software to be accessed by more than one users. This will cause identification and authentication problem because different users use different tokens and protocols, that may cause interpretability problems[7].

2.1.5 Access control

Confidential data can be illegally accessed due to lenient access control. If adequate security mechanisms are not applied then unauthorized access may exist. As data exists for a long time in a cloud, the higher the risk of illegal access.[7][8]

2.2.6 Storage, backup and recovery

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state [1].

Customer may be able to sue cloud service providers if privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.

3. LITERATURE REVIEW

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunication capacity, government surveillance, reliability among others. But the most important between them is security and how cloud provider assures it. Generally, cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect is on performance of computing and for them cloud provides a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. So, as per the perspective of different users, the security point of view is different.

3.1 Security algorithm used in cloud computing

3.1.1 Data security using RSA

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Ada Shamir and Len Adleman, who first publicly described it in 1977.In the work proposed by Parsi Kalpana and Sudha Singaraju, they are using RSA algorithm [1] to encrypt the data to provide security so that only the concerned user can access it.

RSA is one of the widely used encryption algorithm used to provide security to data. Here we are making a provision that only concerned users can access the data, so that it avoids the unauthorized users to access the data. Firstly, the data of users is encrypted and stored in secure place called cloud. When a request came for the data, the request goes to cloud provider. Authentication is done by the cloud provider. If correctly authenticated, provider delivers the data to requested user. This encryption algorithm consists of public and private key. Public key is made public while the private key is owned by the user who originally has the data.

RSA algorithm mainly consists of three steps:

1. Key Generation

2. Encryption

3. Decryption.

Key Generation:

For the data to be encrypted, key must be generated. Key generation is done between the cloud service provider and user.

Step 1: Choose two prime numbers p and q.The numbers should be of similar bit length.

Step 2: Compute the product of p and q.

Step 3: Compute Ø(n) = (p-1) * (q-1)

Step 4: Choose an integer e, such that $1 < e < Ø(n)$ and greatest common divisor of e ,Ø(n) is 1.

Step 5: Determine d,where d is multiplicative inverse of Ø(n) .

Step 6: e is public key exponent and d is private key exponent.

Step 7: Public key is (e,n) and private key is (d,n).

Encryption:

The cloud service provider gave the public key to those who want to save data in cloud service provider. Encryption is done to convert plain text to cipher text. User data is mapped to an integer. The data is encrypted and produce the cipher text C. This cipher text is stored in cloud service provider.

Decryption:

Decryption is the process of converting cipher text to original plain text. The user requests the cloud service provider for the data. the cloud provider firstly verifies users authenticity and gave encrypted data C to authorized users. The user then decrypts the data by computing $m=Cd \pmod n$.Using m the user can obtain the original data by reversing the padding scheme.

Advantages:

1. Only authorized user can access the data.

Disadvantages:

1. Encrypts only small amount of data.

3.1.2 Enhanced data security model

This is one of the work proposed by Eman M.Mohamed Hatem S. Abdelkader.[2].The model used three-layer system structure, in which each floor performs its own duty to ensure that the data security of cloud layers.

First layer: Used for two factor user authentication.

Second layer: Used for user data encryption using one symmetric algorithms. Also provides privacy protection.

Third layer: Used for recovering the data, depends upon the speed of decryption.

Software is implemented with two factor authentication. This is used to compare different encryption algorithm and provide the most suitable algorithm for cloud infrastructure. This software provides to cloud service provider the most suitable algorithm for platform. This ensures security for user data and also retrieves faster.

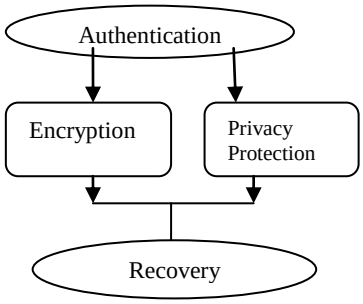

Figure 1: Cloud computing data security model

In this method they made a software to cloud provider with two factor authentication. It compares eight modern encryption algorithms. Based on this it select the most suitable encryption algorithms for each cloud infrastructure. This method makes available the most appropriate algorithm by making some statistical tests. Finally, by this evaluation we ensure that data retrieve faster to the user and ensure security of user data.

In addition, we make software to the cloud user. This software allows user to choose between eight encryption algorithms to ensure data security. This software gives the cloud user some advices to select the most security or most security and faster algorithm that suitable to its cloud infrastructure.

The proposed software solves some problems. This software encrypts and protects data by using the highest encryption algorithm. The software implements strong API access control, by using two way Sign up for Amazon web service to create an account authentications. This software ensures the protection algorithm is highest security algorithm to satisfy the user, by using NIST statistical tests. Ensures faster retrieval, when using faster encryption/decryption algorithm. We also compare between eight encryption algorithms based on speed of encryption to achieve faster recovery.

3.1.2.1 Selecting the highest encryption algorithm

We have 128 sequences (128-cipher text) for each eight encryption algorithm. We compare between 8 encryption methods based on the P-value, Rejection rate and finally based on time consuming for each method. The P value represents the probability of observing the value of the test statistic which is more extreme in the direction of non-randomness. The higher P-value the better and vice versa with rejection rate, the lower the better.AES is the highest security

encryption algorithm based on the NIST test results (based on the P-value or rejection rate).

Advantages:

1) AES is the highest security encryption algorithm.

2) Use blowfish or DES or AES which take less time to encrypt the data than others and ensures that data retrieves faster.

3.1.3 Privacy protection scheme

This architecture selects the protection mechanism in the top half by determining a composition of encryption algorithm and the division numbers to protect user's data. The bottom half protects the data flow and will be protected by implementing system selecting security composition. The system contains four major components – Privacy Analysis, Quantification Models, Data Division, and Data Protection Procedure[4].

The work proposed by I-Hsun Chuang,Syuan-Hao Li,Kuan-Chieh Huang,Yau-Hwang Kuo[4] is that the privacy analysis analyzes user-demand privacy requirement and collects the update frequency of key which is used to encrypt data. The quantification models includes the security and speed aspects. The Data Division is a concept that is used to make data more secure. The Data Protection Procedure is the kernel function, and its major goal is obtaining the composition of encryption algorithm and number of division with maximizing performance in satisfied users privacy requirement.

Privacy Requirement: The data stored in cloud will be like email, video, image, and etc. Each data type has different importance degree for the user in the cloud. It includes different numbers of sensitive information. To ensure confidentiality to data encryption algorithm and data division is composed. If the same strong security composition is used to secure data, it would affect the quality of cloud services. If user requires unimportant data from cloud this high encryption algorithm would affect the service. If weak encryption was used to provide the protection, it would make user's important data insecure and can be revealed. [4]

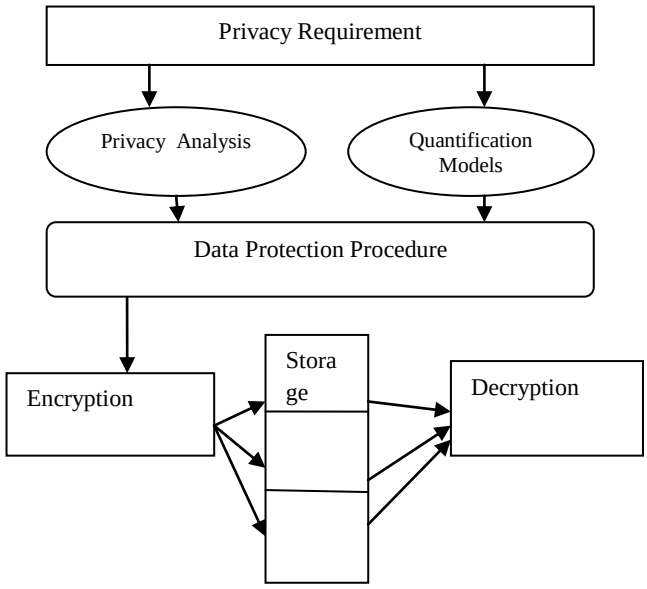

Figure 2: Cloud Secure Architecture [4]

Privacy Level: It has three privacy levels.

1) Speed level: In this level there are no information which are sensitive. Here users use weak encryption composition to obtain higher performance.

2) Hybrid level: Here data include some sensitive information. If weak encryption is used, there is a chance that data will be disclosed if weak encryption algorithm is used.

3) Security level: Here data contains the most important information. User only need to protect the data and not bothered about the performance.

Data Division: Data division is done only after encrypting the data. Although it is assumed that data will be able to obtain by attacker in cryptography, the advantage of this method is making data more secure, because the data is encrypted to cipher text and divided into many parts, and the data can be decrypted only by collecting all of division parts. Some of cloud applications are distributed storing the same data in different storages to make the execution more effective in speed aspect. If attackers cannot take any of all division parts by hacked the storing servers, they cannot recover the encrypted data to crack [4].

Quantification Models: Security and Speed Quantification models are used to evaluate the CPU consumption of encryption algorithms.

Data Protection Procedure: The major goal of this phase is obtaining the optimal composition of encryption algorithm and number of division. The procedure is divided into three phases – preparation, selection scheme, and data processing [4].

1) Preparation: In this phase, gathers the result of analysis from privacy analysis component and the quantification data from quantification models.

2) Selection Scheme: Our selecting principle is finding the composition for expected maximum performance. Because the delay time of encryption depends on encrypted data size Bi and available computing power RCPU, the large encrypted data size or poor computing power will increase the delay. The delay time of network transmission is depended on transmitted data size and available network transmission rate , and data division allows us to keep one part division in local.

3) Data Processing: First we check the state of data. If the data is in form of plain text, then we need to encrypt the data in order to protect confidentiality of data. A Data Encryption Key will randomly generate and the data is encrypted by the key. If the data is cipher text we need to decrypt the data for using by cloud services. The encryption algorithms of stronger encryption algorithm will cause more performance overhead. The number of data division is depended upon the encryption algorithm, if the data require much stronger we divide it into more number of parts, which means stronger [4].

Advantages:

1) Reduces performance overhead

2) Provides confidentiality for users data.

Disadvantages:

1) How the division of data is done is not described here.

2) Data is divided into many parts after encryption and stored on different servers, and if data stored on one of the server is lost it creates problem

4. COMPARISION OF ENCRYPTION ALGORITHMS

Algorithms like: RSA, DES, AES, Blowfish have been used and comparative study among them have also been presented to ensure the security of data on cloud [5] by Rachna Arora, Anshu Parashar. DES, AES, Blowfish are symmetric key algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM. Blowfish was designed by Bruce Schneier in 1993, expressly for use in performance constrained environments such as embedded system. AES (Advanced Encryption Standard) was designed by NIST in 2001. RSA is a public key algorithm invented by Rivest, Shamir and Adleman in 1978 and also called as Asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes.

4.1 AES algorithm

AES is based on the Rijndael cipher[5] developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process[6] .Rijndael is a family of ciphers with different key and block sizes.AES-128 used at client level for data encryption before data is transmitted to the cloud application provider. Then, since application uses SSL as well and an additional point of encryption is applied during data transmission. The data is stored as encrypted on the company servers, along with the public key that is in turn encrypted with a hash of the users password. As AES is used widely now-a-days for security of cloud. Implementation proposal states that First, User decides to use cloud services and will migrate his data on cloud. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best specified services offered by provider. When migration of data to the chosen CSP happens and in future whenever an application uploads any data on cloud, the data will first encrypted using AES algorithm and then sent to provider. Once encrypted, data is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anywhere on cloud. This can be integrated without any changes to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user‘s premises. This encryption protects data and keys and guarantees that they remain under user‘s control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for a wide range of applications.

4.2 DES algorithm

The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm. The strength of DES lies on two facts:

The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.

The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

4.3 Blowfish algorithm

Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard now receives more attention.Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms .Blowfish encrypts 64 bit blocks with a variable length key of 128-448 bits. According to Schneider, Blowfish was designed with the followings objectives in mind:

Blowfish is known to be susceptible to attacks on reflectively weak keys. This means Blowfish users must carefully select keys as there is a class of keys known to be weak, or switch to more modern alternatives like the Advanced Encryption Standard. Blowfish suits applications where the key remains constant for a long time (e.g. Communications link encryption), but not where the key changes frequently (e.g. Packet Switching).

AES considered as best in terms of security and execution time and memory usage is less compared to other algorithms.

Table 1: Comparison of Algorithms [5]

Characteristics	RSA	AES	DES	Blowfish
Key Size	1024 bits	128,192,256 bits	56 bits	32-448 bits
Keys Used	Public key for encryption &private key for decryption	Same key for encryption & decryption	Same key for encryption & decryption	Same key for encryption & decryption
Security	Secure for user only	Secure for user and provider	Secure for user and provider	Secure for user and provider
Execution Time	Time required	Faster	Faster	Less time than RSA

5. CONCLUSION

Analysed different methods for data security in cloud. Various encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES, DES, Blowfish and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers. Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, it has been found that AES algorithm uses least time to execute cloud data. Blowfish algorithm has least memory requirement. DES algorithm consumes least encryption time. RSA consumes longest memory size and encryption time. The future scope of this work is to find out an efficient algorithm to make the data secure by combining homomorphic encryption and MD5 algorithm and use some compression algorithm to protect the data.

6. REFERENCES

[1] Parsi Kalpana,Sudha Singaraju. 2012 Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4.

[2] Mohamed,E.M. , Abdelkader,H.S. , El Etriby,S. 2012 . Enhanced Data Security Model for Cloud Computing. 8th International Conference on Informatics and Systems.

[3] Deyan Chen,Hong Zhao. 2012.Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering IEEE .

[4] I-Hsun Chuang,Syuan-Hao Li,Kuan-Chieh Huang,Yau-Hwang Kuo. 2011. Effective privacy protection scheme in cloud computing. ICACT.

[5] Rachna Arora, Anshu Parashar. 2013. Secure User Data in Cloud Computing Using Encryption Algorithms (IJERA) Vol. 3, Issue 4.

[6] Mandeep Kaur, Manish Mahajan. 2013. Using encryption Algorithms to enhance the Data Security in Cloud Computing. International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03.

[7] ZiyuanWang .2011.Security and privacy issues within the Cloud Computing‖ ,International Conference on Computational and Information Sciences.

[8] K.Sravani, , K.L.A.Nivedita .Effective Service Security Schemes In Cloud Computing".International Journal Of Computational Engineering Research (ijceronline.com) Vol. 3 Issue. 3

[9] S.Arnold.2009.Cloud computing and issues of privacy.

[10] A Platform Computing Whitepaper. Enterprise Cloud Computing: Transforming IT. Platform Computing, pp6, 2010.

[11] Global Netoptex Incorporated. Demystifying the cloud. Important opportunities, crucial choices., pp4-14. Available: http://www.gni.com [Dec. 13, 2009].