A Survey on Various Cryptographic Algorithms for Security Enhancement

Kranti M. Chaudhari,
M.E Scholar, Computer Engineering Department,
JSPMNTC RSSOER, Pune.

Megha V. Borole,
Assistant Professor, Computer Engineering
Department, JSPMNTC RSSOER, Pune.

ABSTRACT:
Cloud Systems can be used to enable data sharing capabilities and this is an abundant benefit to the user. As Cloud computing is a modern era computing technique that has a grater future and bringing a lot of benefit to the information technology. There are some security requirements when dealing with cloud storage. Cryptography is used to make sure that the data is protected. The various algorithms used for cryptography must fulfill the properties of confidentiality, authentication, availability, and integrity. In this paper, we have discussed on the data sharing services of cloud systems and surveyed on various cryptographic algorithms that are used during sharing data securely over the cloud.

Keywords
Cloud Storage, Cryptographic Algorithm, Data Sharing, Security

1. INTRODUCTION
Cloud computing has become one of the biggest emerging trends for research and innovations. It can be defined as a set of resources or services that are offered to the users of internet. These services and products are provided by cloud service providers. Through cloud computing the service providers deliver almost everything as a service over internet on user demand. The user demands may include operating system, network hardware, storage, resources, software, etc. are shown in figure 1. Each and every different organization is moving its data on the cloud and takes the advantages provided by the providers. Data sharing capabilities are provided by Cloud systems [1, 2] and is very beneficial to the customers. A continuous push is given to IT organizations, to enlarge their data sharing capabilities. A survey by InformationWeek [3] says, nearly all organizations share their somewhat 74% of data with customers and 64% with suppliers. Nearly fourth of the surveyed organizations considered data sharing as top priority. These organizations are benefitted with high productivity due to data sharing. Social Networking Services are playing an important role to idolize data sharing capabilities. Facebook is one of a biggest example of data sharing social network. It benefits the user with numerous [4] abilities to share photos, videos, information and events, etc.

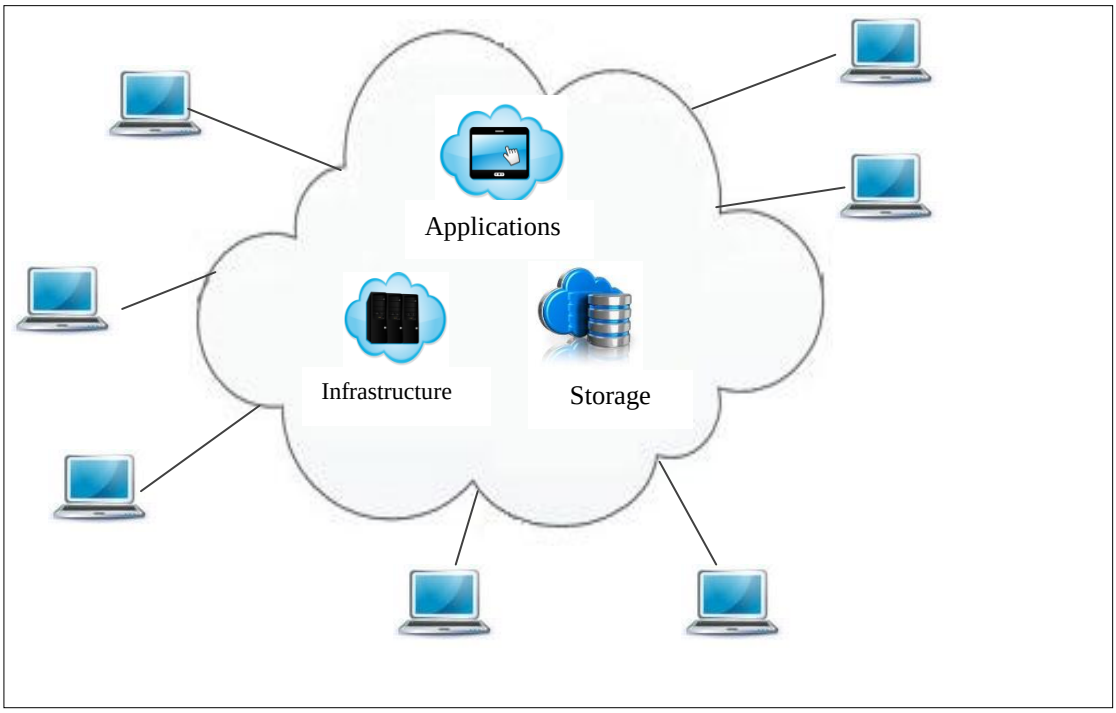

Figure 1. Scenario of Cloud Computing

Google Docs provides data sharing capabilities as groups of students or teams working on a project can share documents and can collaborate with each other effectively. This allows higher productivity compared to previous methods of continually sending updated versions of a document to members of the group via email attachments. Also in modern

healthcare environments, healthcare providers are willing to store and share electronic medical records via the Cloud.

The organizational data is of very important. So there is a crucial need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three important points namely: Availability, Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms, which are: a) Symmetric-key algorithms b) Asymmetric-key algorithms and c) Hashing algorithms. The integrity of data is ensured by hashing algorithms.
Cryptography of the data is nothing but the amalgamation of the contents of data, in such a way that, it is unreadable, invisible or meaningless during transmission over the links. The data contents may include text, images, audio, video, etc. This process of hiding of data is also known as encryption. The main objective of cryptography is to shield the data against the intruders. Once the user receives the encrypted file/data, it needs to be again converted into readable, visible, meaningful format. The contrary process of getting back the original meaningful data is known as decryption. The process includes the restoration of the original data. For the encryption technique, there are various algorithms namely, symmetric-key algorithms and asymmetric-key algorithms.

2. THEOROTICAL BACKGROUND

2.1 Data Sharing in the Cloud

Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organizations aiming to gain profit. Formerly, many people viewed computer as "impersonal giants" who threatened to cut jobs of many people through automation. However, in recent times, it has been welcomed by a huge number of people as it has become significantly social [5]. It is thus not surprising that more and more people are demanding data sharing capability on their phones, computers and even recently Smart TVs.
People always like to share information with one another. They may share it with friends, family, colleagues or the world; thus gaining benefits through sharing data. Some of the advantages include:

2.1.1 Higher Work Rate:

Many business and organizations are getting more productive work done and making a successful alliance with other organizations. Sharing of data has become a key for satisfying the business goals. Many healthcare centers, hospitals are also benefited from data sharing and this has led to the lowering of healthcare costs [6]. Students also gain benefits, when working on group projects, as they are better able to combine with members and get work done more efficiently.

2.1.2 Entertainment:

People of different age groups, can connect with friends, family and colleagues to share their experiences in life. Employees in an organization also use social sites like Yammer, to share their experiences. Sites like YouTube are used for sharing videos, and Flickr is used to share photos. Social data sharing generally provides people with a rich experience as the sharing of personal information can provide people with deeper and stronger relationships.

2.1.3 To share opinions:

People also share information with others, to voice an opinion because many people like to be heard, and hence use social networking sites to stimulate their opinions. Use of social networking sites such as Facebook, Twitter and YouTube to raise awareness about real issues in the world are done nowadays. Although, some campaigns have led to violent protests, online campaigns usually inform people of issues and encourage people to help a cause.

The furtherance in cloud computing has now lead a need for implementing data sharing capabilities in the cloud. Due to the ability of sharing data via cloud, several benefits are manifold. Organizations and business are gaining a huge benefit by outsourcing their organizational data on the cloud. The employees in the organization are also benefited with data sharing capability. They share their work and combine with their co-worker while also working at home or other locations. Workers do not need to worry, as the work is already uploaded to the cloud. With social users, the ability to share files, including documents, photos and videos with other users provides great benefit to them. People use many different mega upload website, to upload their files. But, if these mega upload websites halt, may affect millions of cloud users around the world [7]. The reason for shutting the websites is the illegal content sharing, such as pirated films, full television shows, etc. This represents the strong need for sharing data over the Cloud. Health care center are also benefited by the data sharing service provided by the cloud [6]. Data sharing is also on a great focus for research data [11]. According to the author in [12], many researchers are using this facility in order to speed up the pace of scientific discovery. Financial institutes now days are also using data sharing for better customer support [13].

As with every positive point there is a negative point. There are some problems with data sharing in the Cloud. The data sharing capability is snagged back with privacy and security issues. Cloud is always open to many privacy and security issues, which makes the users of the cloud to adopt secure data sharing techniques to share data over the cloud. In the next subsection 2.2, we shall discuss the requirements of secure data sharing in the cloud.

2.2 Requirements of Data Sharing in the Cloud

The imperative need to be paid attention while sharing data in the cloud is that, only the authorized users of the cloud should be given access to cloud storage. Only the sanctioned users are allowed to use the facilities of the cloud storage. We shall see the ideal requirements of sharing data in the cloud storage below:

2.2.1 Only the owner of the data should be able to specify a group of other users, which are allowed to view shared data.

2.2.2 On specifying the group, any member of the group should be able to gain access to the shared data anytime, anywhere without the data owner's intercession.

2.2.3 No one other than data owner and the members of the predefined group should gain access to the data. The Cloud Service Provider also doesn't get the access to the shared data.

2.2.4 It is in the hands of the data owner, to revoke the access of the data from any member of the group.

2.2.5 The data owner can also add new members to the group.

2.2.6 No member of the group should be allowed to revoke rights of other members of the group or join new users to the group.
2.2.7 The data owner should be able to specify who has read/write permissions on the data owner's files.

2.3 Security Requirements of Data Sharing in the Cloud

Enterprise applications and data are moving into cloud, and this fact is the reason for the popularity of cloud computing. But the lack of security is the major obstacle for cloud adoption. Hence, there are some security and privacy requirements that should be taken into consideration while dealing with cloud storage. Paying attention to these requirements and using them in cloud architecture, can make many cloud users to adopt and cuddle Cloud technology. These essential requirements are as below:
2.3.1 Data Confidentiality: The basic meaning of confidentiality is to restrict the unauthorized user from gaining access to legal data. At any given time, the unapproved users (including the Cloud), should not be able to access data. The shared data should always remain confidential during the transit, and at the rest on backup media. The authorized user should not be disturbed while gaining their rights to access the data. There are two basic approaches to achieve data confidentiality, physical isolation and cryptography. Encryption should be used before the data is uploaded to the cloud.
2.3.2 User revocation: Whenever a user is repealed from the access rights of the data, he/she must absolutely have no rights to access the data at any given time. The user revocation must not affect the authorized user's rights in the group for the purpose of efficiency.
2.3.3 Integrity: The integrity of the data is lost, when it has been modified by the intruder in the network, before the data reaches the destination. Loss of message integrity is not accepted by any cloud user. A modification sensitive data must be checked for any alterations by unauthorized user. In this process, the data is protected from malicious modification. In the cloud system, preserving information ntegrity means by data integrity. As data is of at most importance in cloud computing services, keeping its integrity is a basic task. Data provides a basis of services such as Software as a service, Platform as a service, Data as a service, etc. Digital Signature is a widely used technique for maintaining data integrity. There are also other techniques such as, RAID-like strategies, hashing techniques, message authentication codes and so on.
2.3.4 Scalability and Efficiency: Many of the cloud users are extremely large at times, and it is completely unpredictable how many users can join and leave the cloud system. Thus, the cloud system and its architecture must be scalable enough and it should also be efficient.
2.3.5 Collaboration between entities: While considering data sharing methodologies, it is essential that even when certain entities collaborate, they should still not be able to access any of the data without the data owner's permission. The prior works on data sharing issues had not considered this problem, however collusion between entities can never be written off as an unlikely event.
2.3.6 Availability: Ensuring cloud users that they can use the cloud services at any place and at any time is known as providing the advantage of availability to the cloud users. Hardening and redundancy are the known strategies used for enhancing the availability of the cloud system. The data owners are always ensured to their data and to the compute resources.

3. REVIEW ON CRYPTOGRAPHIC ALGORITHMS

Security has always being an important term in all the fields. As the paper is discussing on cloud storage systems, we shall consider the security required to the data that is stored on the cloud. Cryptography has come up as a solution to this security issue.
Many different techniques and encryption algorithms are required to preserve the shared data. There are various cryptographic algorithms as shown in figure 1.1. Table 1.1 shows the comparison between some of the algorithms and we shall discuss some of the cryptographic algorithms below.

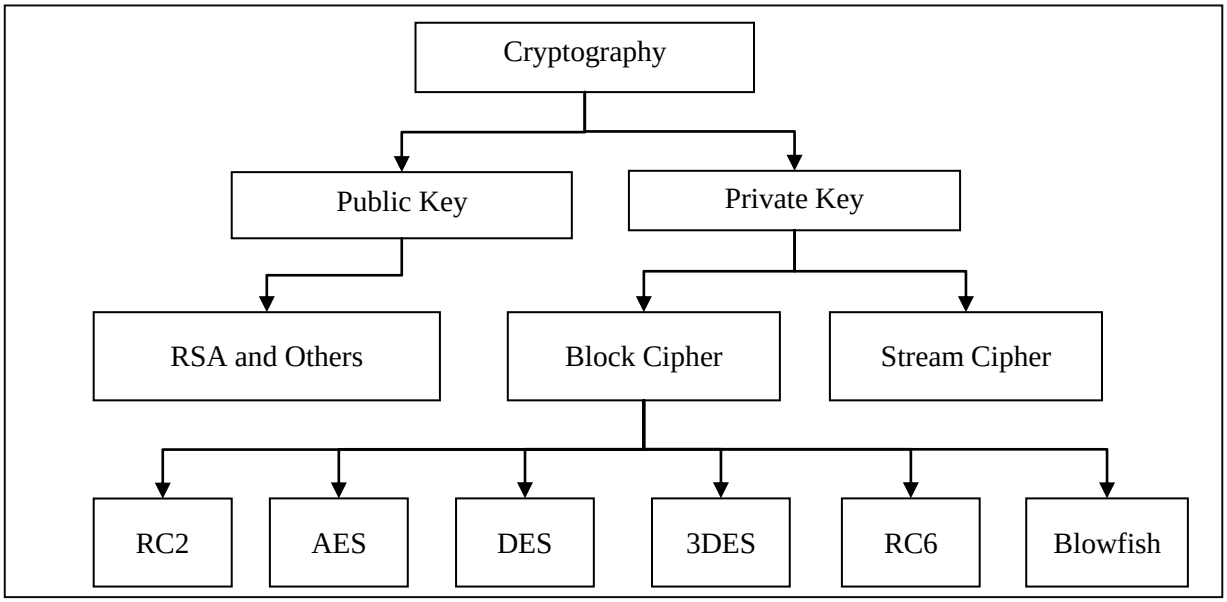

Figure 2. Types of Cryptographic Algorithms

3.1 Advanced Encryption Standard Algorithm

The Advanced Encryption Standard (AES) algorithm is not only known for security but also for its higher speed. The hardware and software implementation are also comparatively faster in speed. This algorithm is based on Rijandael and it is similar to DES algorithm that uses substitution and permutation along with multiple rounds. The key size and block size are responsible for changing the number of rounds. AES can be devised on several platforms such as small devices. All the operations in this algorithm involve complete bytes for effective implementation. Three different key lengths such as 128, 192 and 256 block size are supported by AES.

3.2 Data Encryption Standard Algorithm

The purpose of the Data Encryption Standard (DES) algorithm is to supply a standard method for protecting the crucial data. Many industries and organizations had adopted this algorithm for use of security purpose. In this algorithm, the plain text is encrypted into 64bits and it also yields 64bits of cipher text. We can also protect sensitive commercial and unclassified data by using DES algorithm. There is a same key used for both the operations encryption and decryption [8]. A different variant of DES algorithm is known as triple DES which uses two keys and three stages.

3.3 RSA Algorithm (Rivest-Shamir-Adleman)

The Rivest-Shamir-Adleman (RSA) algorithm is very widely used technique for encryption process and creation of digital certificates. This algorithm is a type of public key algorithm and is named after the inventors name which are Ron Rivest, Adi Shamir and Leonard Adelman respectively. The intensity of factoring large number may affect the security provided by the RSA algorithm. There are two different keys used in this algorithm and they are public key and private key. These two keys are functions of a pair of large numbers. As this algorithm is based on arithmetic modulo large numbers, it can be slow in compelling environments [9].

3.4 Elliptic Curve Cryptography Algorithm

ECC was developed by Neil Koblitz (University of Washington) and Victor Miller (IBM) in 1985. It is a public key encryption technique based on discrete logarithms which is used to create efficient, faster and smaller cryptographic keys. ECC generates keys by using the elliptic curve equation rather than traditional systems.

3.5 ElGamal Algorithm

ElGamal algorithm is based on the difficulty of solving the discrete logarithm problem. It is an example of public-key cryptosystem. This algorithm can be used for both encryption and decryption process. The security of the ElGamal scheme relies on the difficulty of computing discrete logarithms over GF(p), where p is a large prime. Prime factorization and discrete logarithms are required to implement the RSA and ElGamal cryptosystems. The ElGAmal algorithm is used for both encryption and signature algorithms. Using this algorithm the user not only can encrypt the data but also for digital signature where the security lies on the challenge of divergence logarithm in finite domains [10]

4. CONCLUSION

Many applications are relying on the technology known as Cloud computing. Cloud storage is playing a very crucial role for many organizations and industries. Any application relying upon an emerging technology should always consider the different possible security and privacy requirements. Failure in implementing the security techniques may probably lead to great loss for the organizations. We have discussed the need for sharing the data on the cloud and also stated the security requirements for sharing data onto the cloud. Proper survey discussed on cryptographic algorithms in the paper, may help many cloud users to make proper choice.

Table 1. Comparison between Cryptographic Algorithms

Factors	Advanced Encryption standard	Data Encryption standard	RSA Encryption	ElGamal Encryption
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm	Asymmetric Algorithm
Key Size	128,192,256 bits	56 bits	>1024bits	1024 bits
Key used	Same key used for encrypt and decrypt	Same key used for encrypt and decrypt	Different key used for encrypt and decrypt	Different key used for encrypt and decrypt
Ciphering and Deciphering key	Same	Same	Different	Different
Ciphering & Deciphering Algorithm	Different	Different	Same	Same
Scalability	Not Scalable	Scalable	Not Scalable	Good Scalability
Security	Excellent secured	Not secured enough	Least secure	Enough Secured
Simulation Speed	Faster	Faster	Faster	Faster
Inherent Vulnerabilities	Brute Force Attack	Brute Force, Linear and differential cryptanalysis attack	Brute Force and Oracle attack	Meet-in-The middle attack
Hardware and Software Implementation	Faster	Better in hardware than in software	Not efficient	Faster and efficient

5. ACKNOWLEDGMENT

We honestly grateful to all those referees and security experts, for their valuable guidance and suggestions during grounding of this research article The Success of this survey would have been undefined without the help and guidance of a dedicated group of people in our institute and our Director of JSPM's NTC Pune.

6. REFERENCES

[1] Mell P, Grance T (2012) The NIST definition of cloud computing. NIST Spec Publ 800:145. National Institute of Standards and Technology, U.S. Department of Commerce. Accessed on Oct 2012.

[2] Wikipedia definition of Cloud computing (2012). Source: http://en.wikipedia.org/wiki/Cloud_ computing. Accessed on Oct 2012

[3] HealeyM(2010) Why IT needs to push data sharing efforts. Information Week. Source: http://www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/225700544. Accessed on Oct 2012

[4] Gellin A (2012) Facebook's benefits make it worthwhile. Buffalo News.

[5] Scale ME (2009) Cloud computing and collaboration. Library Hi Tech News, pp 10–13.

[6] Ratley N (2012) Data-sharing 'would benefit patients'. The Southland Times.

[7] Galvin N (2012) File-sharing service users in cloud over access to data. The Age.

[8] Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard Algorithm". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013, pp. 264.

[9] Qing LIU, YunfeiLI,Tong LI, Lin HAO, "The Research of the Batch RSA Decryption Performance", Journal of Computational Information Systems 7:3 (2011) 948-955.

[10] Rajan S. Jamgekar, Geeta S. Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE)ISSN: 2319–6378, Volume-1, Issue-4, February 2013.

[11] Melis RJF, Vehof H, Baars L, Rietveld MC (2011) Sharing of research data. Lancet 378(9808):1995.

[12] Feldman L, Patel D, Ortmann L, Robinson K, Popovic T (2012) Educating for the future: another important benefit of data sharing. Lancet 379(9829):1877–1878.

[13] What's in it for me? the benefits of sharing credit data (2011). Banker, Middle East.