International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-6, Issue-8, August 2020
ISSN: 2395-3470
www.ijseas.com

A Review on Enhanced Crypto Security in Different Fields on Cloud Storage Platform

Dr.R.Malathi Ravindran[1], Mr.P.Prabhakaran[2]

[1] Associate Professor, Department of Computer Applications,
NGM College, Pollachi, Coimbatore, Tamilnadu, India.

[2] Research Scholar, Department of Computer Science,
NGM College, Pollachi, Coimbatore, Tamilnadu, India.

Abstract

Cloud Computing – a relatively recent term, defines the paths ahead in computer science world. Being built on decades of research it utilizes all recent achievements in various fields. Cloud Computing has become a scalable services consumption and delivery platform in the field of Services Computing. Cloud Computing is a better way to run your business. Data storage security refers to the security of your personal or official work on the storage media. Range of users stores their data on Cloud Server and with passage of your time Cloud Computing grows in numbers of time. Information should not be taken by the third party therefore authentication of consumer becomes a compulsory task.

Security doesn't solely mean Arcanum protection or adding extra firewalls or hide the information. It additionally suggests that having complete information concerning your data or information i.e. wherever hold is on on-line or offline and who all read it. Before proposed the scheme, the definition of Cloud Computing and transient discussion to beneath Cloud Computing is given. Then discusses cryptographic algorithm to employed in cloud & propose the new theme for offer the safety to cloud storage. Cloud Computing are use in Entertainment, Medical, Military Operations, Security issue, Business and finance etc [1].

This paper describes the use of Cloud Computing in various fields with cryptographic algorithms.

Keyword: *Cloud Computing, Cryptography Algorithms, Security, Data Storage*, Public & private Cloud.

[1] Introduction

Data Security is a major field in Networking. Data security has been a leading issue in the Information Technology arena because as users we don't want anyone to hinder our privacy and as developers we don't want anyone to use our work as their own. The Cryptographic Cloud Computing and Storage has two basic parts i.e. Cryptography and second one is Cloud or Network Storage [5]. The Cloud Computing is Internet based computing where virtual shared server provides software, infrastructure, platform, devices and other resources. Cloud Computing has become a scalable services consumption and delivery platform in the field of Services Computing [11].

Cloud Computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).

Security Issues Face by Cloud Computing are

- Data Access Control
- Data Integrity
- Data Theft
- Data Loss
- Privacy Issues
- Security problems in supplier level

Encryption should be properly used and the crypto algorithms include AES, RSA and DES [2]. The secured cloud storage at least should provide the following

- C**onfidentiality:** The cloud storage provider does not learn any information about customer data
- **Integrity:** Any unauthorized modification of customer data by the cloud storage provider can be detected by the customer while retaining the main benefits of a public storage service:
- **Availability:** Customer data is accessible from any machine and at all times
- **Reliability:** Customer data is reliably backed up
- **Efficient retrieval:** Data retrieval times are comparable to a public cloud storage service
- **Data sharing:** Customers can share their data with trusted parties.

In this paper, the crypto cloud storage in different fields are reviewed and identified why the cloud storage is need for those fields.

[2] Cloud Storage in Different Fields

The following are the different fields which using cloud storage mostly,

- Business
- Medical Fields
- Education
- Information Technology
- Finance and Banking
- Telecommunication
- Agriculture
- Online Entertainment

[3] Benefits of Cloud Storage

Cloud storage is one of the primary uses of Cloud Computing. With the cloud storage, data is stored on multiple third party servers, rather than on the dedicated servers used in traditional networked data storage. When storing data, the user sees a virtual server that is; it appears as if the data is stored in a particular place with specific name. But that place does not exist in reality. It is just a pseudonym used to reference virtual space carved out of the cloud. In reality, the user's data could be stored on any one or more of computers used to create the cloud.

The actual storage location may even differ from day to day or even minute to minute, as the cloud dynamically manages available storage space. But even though the location is virtual, user sees a static location for his data and can actually manage his storage space as if it were connected to his own pc.

The goal to use elliptic curve cryptography (ECC) is that it fits well for an efficient and secure encryption scheme. It is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for equivalent security [3].

- **Authentication**

User must be authenticated to access the service from cloud. The commonly used security mechanism for data access is username and password pair. User provides the username and password pair to cloud service provider and then cloud service provider checks the authenticity of the user. If user is authorized, cloud service provider will load cryptographic model (E-Module) to the client end that is responsible for cryptographic operation.

- **Operation**

Cryptographic module asks for pin number to generate the secret key.

- **Encryption**

The data that has to stored in a cloud cannot be stored in plaintext format due to security reason so it must be transformed into an encrypted format. Cryptographic module use the secret key to encrypt the user's data that needs to store on cloud.

- **Decryption**

This method deals with the decrypting the data after downloading from cloud. On user requests to download data stored on cloud, server will send the data in encrypted format. After arrival of data at client end Cryptographic module will decrypt it and original file is available to client.

[4] Security Methodology applied in different fields for cloud storage

Business

Cloud Computing is both a business delivery model and an infrastructure management methodology. The business delivery model provides a user experience by which hardware, software and network resources are optimally leveraged to provide innovative services over the Web, and servers are provisioned in accordance with the logical needs of the service using advanced, automated tools [1]. The cloud then enables the service creators, program administrators and others to use these services via a Web-based interface that abstracts away the complexity of the underlying dynamic infrastructure.

Medical Fields

Within a hospital, indeed within the majority of medical practices, patient charts and medical histories are often kept within a computer system of some kind. In a hospital this is especially useful as the sheer number of patients within the building at any one time can be daunting. Cloud Computing can help facilitate easier access and distribution of information among the various medical professionals who may come in contact with each individual patient. In current vast hospitals, servers are connected, but the sheer amount of information and computers that must be connected is staggering. A cloud based system will improve information sharing by allowing everything to be hosted in the same place, allowing a doctor to input test results in the lab, instantly updating the chart of a patient in a completely separate wing. Similarly, it can allow offsite buildings and treatment facilities like labs, doctors making emergency house calls and ambulances, to have and update information remotely, instead of having to wait until they can access a hospital computer.

Cloud Computing can also be greatly beneficial to private practice doctors as well. The mobility option in this case may be even more important than in hospitals. While you may see a patient for a yearly physical, or to treat non-emergency illnesses, a sudden injury or disease will send that patient to an emergency room, not your office. With a cloud based server, you could integrate your own system with the local hospitals, and when a patient of yours is admitted, your own files could be updated immediately. Similarly, if you were to go and treat this patient in said hospital or in their home for whatever reason (such as a home birth) you‟d not only be able to immediately and remotely access their records, but request assistance or, in the case of the birth, immediately add the new patient. computing is a relatively new way to host information, and as such, the benefits for every individual business isn’t always immediately obvious, but for a field like medicine, it’s difficult to find any downsides.

Education

It is one of the fastest-growing industries in the world. The need and demand of education never goes down. Cloud Computing in education opens avenues for better research, discussion, and

collaboration. It also provides a software desktop environment, which minimizes hardware problems. Cloud Computing also enables classes to be run on remote locations.

The benefits of Cloud Computing are that outside entities might be more sophisticated at managing personal data. These entities may be able to manage data more inexpensively and effectively than the educational institution could do itself. In many cases, Cloud Computing providers can provide better security than the educational institutions can.

The risks of Cloud Computing are that educational institutions no longer have as much control over the personal data. They must rely on the Cloud Computing provider to have the appropriate practices and policies to ensure that data is properly maintained, handled, used, or disclosed.

One risk is that a Cloud Computing provider can outsource some functions to countries that have little to no legal privacy protections. In one instance, a university medical center outsourced transcription of its medical records to a company in California, which then subcontracted with a person in Florida, who subcontracted with a person in Texas, who ultimately subcontracted with a person in Pakistan. The person in Pakistan wasn't paid by the person in Texas, so she wrote to the medical center and threatened that she would expose all the records unless the medical center got involved and made the Texas person pay. This example illustrates how easy it is to lose control over information when it is outsourced.

There are benefits and risks to Cloud Computing, but the benefits can be enhanced and the risks greatly reduced if educational institutions take care and vigilance in selecting Cloud Computing providers and in monitoring the relationship to ensure that the provider is adequately protecting the data.

Information Technology

The IT industry thrives on information and Cloud Computing provides the perfect platform for testing of new software and techniques. The use of Cloud Computing is rapidly growing, and so is the literature on the technical issues of implementation. Our knowledge of the managerial implications of Cloud Computing, however, still lags far behind. This paper examines the phenomenon of Cloud Computing, places it in the context of other major changes in Information Technology (IT) and explores the potentially revolutionary transformations and challenges it brings to management. The paper starts by analyzing the IT pendulum of centralization and decentralization along a few major periods:

- Mainframes and batch transaction processing (e.g. financial systems), fully centralized IT, end-users receiving outputs;
- Mainframes and online transaction processing, IT still centralized but end-users interacting with the system (e.g. ATMs, online reservation systems);
- PCs, end-user computing and internal business decentralization;
- Web 1.0, mass decentralization and full access to e- mail, home banking, online shopping, social interaction, etc.;

- Web 1.0 plus outsourcing, where the front end of the business moves to the web, with non-competitive transaction processing systems and support being commoditized and located anywhere; and

- Web 2.0 plus Cloud Computing, with virtualized organizations using web 2.0 tools, net PCs, mobile technology and Cloud Computing services.

Managerial implications of Cloud Computing and conclude by arguing that Cloud Computing represents a major IT change, transforming the way IT professionals work, and also a potential managerial revolution, with a fundamental change in how managers conceptualize and conduct business.

Finance and Banking

As the international market grew so did the need for a more condensed and easier financial reach. Cloud Computing eliminates the need for having a separate banking portal and client database for every location. This means faster and better business.

Despite the slow adoption of Cloud Computing by the banking and financial services industry with security and reliability being the major concerns, financial institutions are quickly resorting to cloud-based services to achieve increased agility and lowered total cost of ownership (TCO). According to IDC, worldwide revenue from public IT cloud services exceeded $21.5 billion in 2010 and is expected to reach $72.9 billion in 2015. There is an emerging trend in which financial institutions are embracing “cloud solutions” as not just a „me- too‟ option, but as solutions that yield competitive advantage due to shorter cycles of time to market for products and services.

Over the years financial institutions typically have been consumers of cloud-based solutions across generic and non-core services like virtualization, datacenter consolidation, storage and disaster recovery. Many financial institutions are either planning or have implemented in-house private clouds for sensitive consumer data and are utilizing the public cloud for generic services. As Cloud Computing capabilities mature and become more reliable, multi-tenancy and hybrid cloud models will drive increased adoption of cloud-based solutions that are focused on core services and achieve cost efficiencies and scalability.

Telecommunication

Telecommunication companies can use Cloud Computing to provide both private and public cloud networks to customers and organizations for domestic and commercial purposes. hen we use Cloud Computing in Telecommunication field so its known as Cloud Communication. Cloud communications are Internet-based voice and data communications where telecommunications applications, switching and storage are hosted by a third-party outside of the organization using them, and they are accessed over the public Internet. Cloud services is a broad term, referring primarily to data-center-hosted services that are run and accessed over an Internet infrastructure. Until recently,

these services have been data-centric, but with the evolution of VoIP (voice over Internet protocol), voice has become part of the cloud phenomenon.

As telecommunication architectures move towards a more cloud-oriented structure, there will be more demand on self- services. This is even more significant in the mobile telecoms where people are now basically utilizing the cloud as the processing power unit for their mobile devices, turning them into high performance utility tools.

Agriculture

Along with a rapid growth of Cloud Computing technology and its deep application in Agriculture Intelligent Information System, Agriculture Industry information security and privacy has become a highlight of the issue about Agriculture Cloud Information System [6]. Encrypting is a conventional information security means, however, hitherto almost all encryption scheme cannot support the operation based on cipher-text. As a result, it is a difficult to build up the corporate and individual information security and privacy-securing in the information system based on Cloud Computing platform. In order to construct the information security and privacy of Cloud Computing infrastructure, down to the practicality of Agriculture Information System the project crew brings forward An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform.

Online Entertainment

Most people come on the internet for entertainment; therefore, Cloud Computing is the perfect place for reaching to a varied consumer base. Cloud-based entertainment can reach any device be it TV, mobile, set top box, or any other form. Better clarity and sound quality gets cloud entertainer more customers.

Televisions have come a far away from their monochromatic ancestors of the 1930's to become the modern age's ultimate home entertainers. Demands and expectations of the consumers have evolved tremendously to put a strain on the traditional mediums of entertainment, i.e. audio and video. Moreover, the advent of internet and has created another dimension in home entertainment – let’s call it "On Demand Entertainment" (ODE). True ODE means consumers will be able to watch, listen, play or read whatever they want whenever they want.

The consumers of Televisions now have options of going on the Internet and search for ODE including (but not restricted to) games, news, video and audio. Internet giants like Amazon, Hulu, Netflix and Youtube have started cutting into Television industry's profits and have become a major force to reckon with in home entertainment segment.

In a parallel development, consumers now want seamless integration and convergence between the new and the old media of entertainment. This expectation has led to innovation in Television industry in the form of IPTV, satellite TV and internet enabled TVs. These technologies

strive to provide ODE as well as try to fulfill the demand for a unified entertainment device. However, true ODE is still a distant dream because of the strain it puts on the storage and computation power of the back-end data centers.

Cloud Computing or internet based computing, which provides on demand storage and compute power to be billed in a pay-per-use basis, comes as a perfect strategic fit to solve the puzzle of ODE. Cloud Computing can provide a solution to the issue of huge requirements in compute and storage to provide true ODE.

[5] Application of Cryptography Algorithm on Cloud Storage

A hybrid computing model enables an organization to leverage both public and private computing services to create a more flexible and cost-effective computing utility:

- The public cloud is a set of hardware, networking, storage, service, and interfaces owned and operated by a third party for use by other companies or individuals [4].
- A private cloud is a set of hardware, networking, storage, service, and interfaces owned and operated by an organization for the use of its employees, partners, and customers.
- In a hybrid cloud environment, an organization combines services and data from a variety of models to create a unified, automated, and well-managed computing environment.

This is the combination of cryptography and fragmentation technique with authentication. The following Fig. described the scheme for cryptographic Cloud Computing & storage. For using that application user need to registered and create the new username/password by running the setup.jar file. User need to enter new username and password in login window and click on login button for access the application.

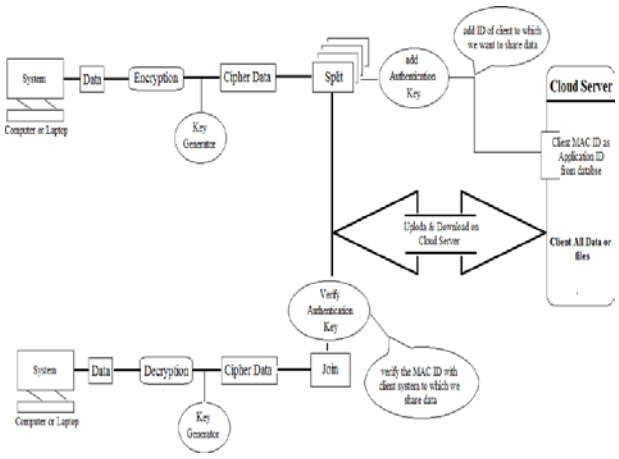

Figure1. Cryptographic Cloud Computing and Storage

The Above scheme illustrate the propose methodology in which we will done the following operations. At first we can encrypt the data using DES algorithm (Data Encryption Standard) and also generate the key which is used to decrypt that data [9].

After that user can convert that cipher data into byte size or split (Fragment) into multiple parts. When we convert any file into byte size or split the file, it is in the unreadable format i.e. it also used as the cryptography technique which is used with the DES Algorithm that increased the strength of that algorithm [8].

After that we add the authentication key i.e. MAC ID of the client system that user wish to share the data. The authentication key is choosing by the user from cloud server where all registered user MAC ID are available. User simply needs to choose the client name from which MAC ID of that client is added as authentication.

No one can identify that MAC ID's because at the registration time we add some string with that MAC & performed the reversed operation on that and stored it into cloud server. In somewhat conditions if unauthorized user successfully accesses that cloud database, it's difficult to identify that MAC ID of client systems. After authentication user share that file or data to on cloud server [10]. We done the same operation in vice-versa manner i.e. first split the original file & add authentication then encrypt one of the parts of spited file.

To get the original data we done the same procedure in reverse order i.e. first download that data files then verify the authentication with client MAC ID, after successfully authentication spited parts of file are joined. After that using the DES key we decrypt the data and get the original file which is in readable format.

[6] Conclusion

After the review of all the base papers, we have identified the applications of Cloud Computing in various fields. And also what are the crypto security algorithms they have applied. In the above study all author have implemented in their own perspective in their own field. The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. We exploit the technique of elliptic curve cryptography encryption to protect data files in the cloud. Two part of the cloud server improved the performance during storage and accessing of data. The ECC Encryption algorithm used for encryption is another advantage to improve the performance during encryption and decryption process.

It is a technology that will be adopted if the areas of concerns like security of the data will be covered with strong mechanism. The strength of Cloud Computing is the ability to manage risks in some particular security issues.

This paper showed the basis of Cloud Computing, and its possibilities of use in the various fields. The concept of Cloud Computing comes from the network diagrams illustrating the Internet as a cloud, where it is not possible, or not important, to know the information path. While the main reasons for adopting services based on Cloud Computing are cost saving, flexibility and start-up speed, there are still doubts about the security guarantees and the portability and integration options offered by this model of services.

Cloud Computing is growing as a new thing and it is the new trend indeed and many of the organizations and big companies are moving toward the cloud but lagging behind because of some security problems. Cloud security is an ultimate concept which will crush the drawbacks the acceptance of the cloud by the big MNCs, companies and organizations [12]. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms.

Based on the study of crypto security on cloud storage in various fields, the author can able to understand that the applications of cryptography algorithms are how used in different fields and how it can be useful for our research field.

References

[1] Manoj Chopra, Jai Mungi, Kulbhushan Chopra, "A Survey on Use of Cloud Computing in various Fields" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, Issue 2, February 2013.

[2] Rohit Bhore, Dr. Rahila Sheikh, "Secure Data Storage Scheme Using Cryptographic Techniques in Cloud Computing", International Journal of Computer Science and Network, Volume 5, Issue 1, February 2016.

[3] Ankita Nandgaonkar, Prof. Pallavi Kulkarni, "Encryption Algorithm for Cloud Computing" International Journal of Computer Science and Information Technologies, Vol. 7 (2), 2016.

[4] Arjun Kumar, Byung Gook Lee, hoonjae Lee, "Secure Storage and Access of Data in Cloud Computing", Conference Paper, October 2012.

[5] Seny Kamara, Kristin Lauter, "Cryptographic Cloud Storage", Conference Paper, January 2010.

[6] Tan, Wen Xue, "An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform", Journal of Software, vol. 9, no. 1, January 2014.

[7] V. Miller. "Uses of Elliptic Curves in cryptography". CRYPT'85, LNCS 218, pp 417-426, 1986.

[8] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[9] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. M. Lee, G. Neven,P.Paillier, and H. Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In V. Shoup, editor, Advances in Cryptology – CRYPTO ’05, volume 3621 of Le/cture Notes in Computer Science, pages 205–222. Springer, 2005.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In P. Ning, S. De Capitani di Vimercati, and P. Syverson, editors, ACM Conference on Computer and Communication Security (CCS ’07). ACM Press, 2007.

[11] Sanjoli Singla, Jasmeet Singh ,”Cloud Computing security using encryption technique”, IJARCET, vol.2, ISSUE 7.

[12] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing”, Department of ECE, Cong Wang, Illinois Institute of Technology.