ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (727-729), Month: April - June 2015, Available at: www.researchpublish.com

Performance Analysis of Cryptographic Algorithms: An Overview

[1]Ms.Anvitha N, [2]Mr.Guruprasad

[1]Student, Dept. of Computer Science and Engineering
[2]Assistant Professor, Department of Computer Science and Engineering
[1, 2] Mangalore Institute of Technology and Engineering (MITE), Karnataka, India

***Abstract*: The increase in the use of computing resources has resulted in the electronic data generation at highest rate. The cloud storage is an easy and cost effective solution for the users running out of storage space at their end. The cloud service provider (CSP) stores user data on to a storage server placed in a data center at remote location. This availability, confidentiality and integrity of the data must be maintained by CSP in order to increase revenue. So the Disaster Recovery as a service (DRaaS) is becoming one of the major areas of interest. The data redundancy is maintained by using geographically dispersed data centers so that data lost from one location can be recovered from another. The data integrity can be achieved by using the cryptographic solutions. In this paper we compare the existing cryptographic algorithms like ECC, RSA with the new Seedblock algorithm and analyse the result.**

***Keywords*: Cloud Service Provider, Disaster Recovery as a Service, Remote Backup Server, Seedblock, main server.**

1. INTRODUCTION

Cloud computing describes the combination of logical entities like data, software which are accessible via internet. National Institute of Standards and Technology defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts and service provider interaction. The cloud computing provides benefits such as cost savings, flexibility, maintenance and mobile accessibility. Most of the business organizations are migrating towards cloud for the betterment of their services and hence achieve their organizational growth along with improved customer revenue.

The cloud service must be accessible from anywhere, anytime without any interruption in the presence of Internet. The natural disasters usually cause physical damage to data centers and hence result in a massive loss of time and money. In order to efficiently serve the customer requirements, the cloud service provider (CSP) must have an effective data backup and recovery technique. This leads to the concept of redundancy of the data, in which the user data will be hosted on remote, geographically dispersed data centers, so even if a disaster hits one geographic region, back up data centers in other geographic areas will continue to operate, allowing the user to have constant access to the data.

The data placed on backup servers at remote location needs security in order to withstand the physical damages as well as the data loss due to intruders. The security can be provided to the data by applying the cryptographic measures before storing it on remote cloud server so that its integrity will be maintained. The Seedblock algorithm [1] is designed to provide security to data stored on remote cloud without using the existing cryptographic algorithms. In this paper we will perform a comparative study about the performance of cryptographic algorithms like ECC, RSA with the Seedblock algorithm.

The rest of the paper is organized as follows: Section II represents literature survey, section III represents proposed plan, section IV represents results and discussion and section V represents conclusion of the paper.

2. LITERATURE SURVEY

Internet has become part and parcel of our lives and the electronic data generation is also achieving its highest rate. This leads to increased usage of storage and computing resources and hence increasing the cost. So the cost effective way is to adopt cloud computing architecture for the day to day activities and the business needs. The cloud provides different services based on customer requirements. The cloud storage is basically "a technique to store, coordinate and protecting the essential data" in a virtual cloud that can be repeatedly accessed by multiple users [2]. The users must have to be authorized on a particular network and they can access the data storage from anywhere at any time. It allows the remote retrieval of the stored files, provides mobility in the work-flow of a company or business and an affordable way of protecting important data. The cloud also enables access to files from any device [3], including mobile phones, tablets and laptops and hence enforces uniform permissions across multiple devices. Cloud storage requires high speed Internet most of the time and the user may find it troublesome to access data when a provider closes its service for maintenance and repair. So the cloud storage systems normally depend on hundreds of data servers to store the same information on multiple machines. This is known as redundancy [5]. Cloud storage is often used as a way to create "backups of data" along with its usage as storage space.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (727-729), Month: April - June 2015, Available at: www.researchpublish.com

Natural disasters devastate communities and destroy lives. Often overlooked is their effect on businesses. Studies show that more than 25% of businesses damaged never recover from disasters like floods, hurricanes, earthquakes, or tornados [4]. Those that do recover are typically the ones that sought comprehensive disaster recovery solutions before a disaster occurred. So the businesses that store their data in the Cloud must have a built-in disaster recovery plan in effect. This is because cloud computing data providers host the user data in remote, geographically dispersed data centers, and hence if a disaster hits one geographic region, back up data centers in other geographic areas will continue to operate, allowing user to have constant access to data.

The process of devising a disaster recovery plan starts with identifying and prioritizing applications, services and data, and determining for each one the amount of downtime that's acceptable before there's a significant business impact. The recovery time objective (RTO) [7] is the time duration between disruptions till restoration of service. The recovery point objective (RPO) defines the amount of data lost after a disaster. Both the RTO and RPO must be minimized to achieve business continuity. The parity cloud service [6] (PCS) is one of the data recovery methodology that provides parity based recovery service which requires a reasonable server side cost and recovery of user data with sufficiently high probability.

3. PROPOSED PLAN

The cloud storage service is not just for those users concerned about running out of space. It is often used as a way to create backups of data. The cloud service provider will maintain the multiple data centers spread over different geographical areas so that user data will be available without loss. The data stored on cloud will be vulnerable to unauthorized access by an intruder. This paper proposes a comparative study on providing security to data using different cryptographic methods.

There are several cryptographic algorithms that are used to provide security to user data by applying encryption mechanism to the user data. In this proposed work we compare the performance of RSA, ECC and Seedblock algorithm [1] and provide an overview about their working. The encryption time includes the key generation, retrieval of file and encrypting the file using the generated key. The decryption time includes the file retrieval, obtaining the decryption key and decryption of the file using the key.

The experiments are conducted in system with Intel® Pentium(R) CPU G2020 @ 2.90GHz × 2 processor with 2GB RAM. The time taken by each algorithm to encrypt the files of different sizes is represented using the graph as shown in Fig.1. The Fig. 2 shows the graph representing the time taken by each of the algorithms for decryption the same files.

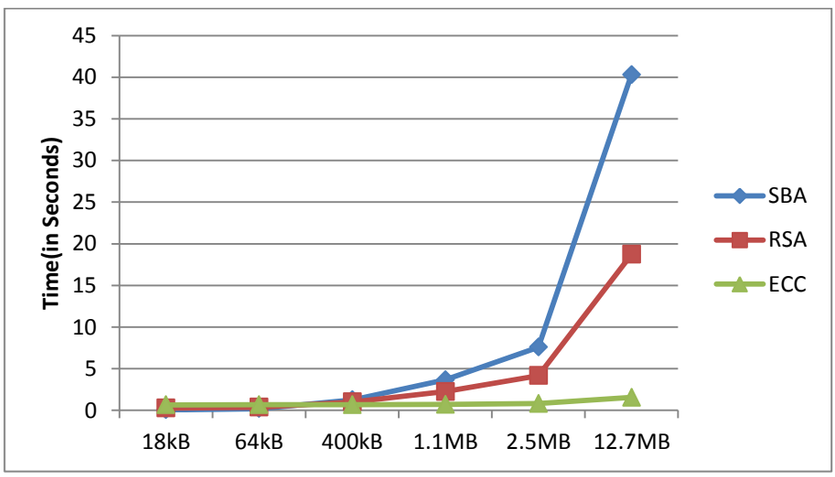

Fig.1 Graph Showing Data Encryption Time

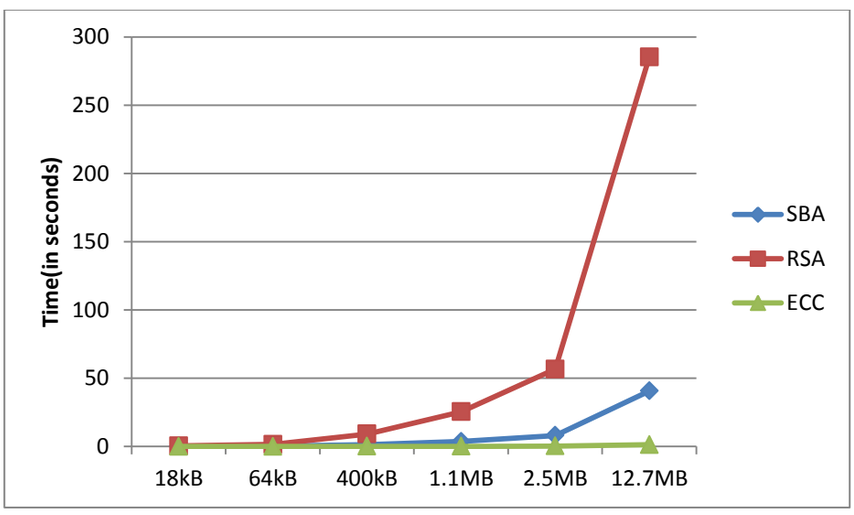

Fig.2 Graph Showing Data Decryption Time

4. RESULT AND DISCUSSION

The experimental results show that the ECC algorithm will work in an efficient manner than the other two algorithms. But the seed block algorithm is simple to implement and it works in a reliable manner with the acceptable encryption and decryption times. So using seed block algorithm is a simple and easy way to achieve security and integrity of user data.

Security is a very important area in cloud computing and there are several methodologies are being developed to achieve the best result. The Seedblock algorithm is one of the simple and easy algorithms that can be used to provide security to user data. But the key used in this algorithm is not secure and an intruder getting access to the key can easily get the data using it. So, there is a need to focus on providing confidentiality and integrity to the key throughout its lifetime.

5. CONCLUSION

The Seedblock algorithm is a simple and easy to implement encryption methodology. The study shows that the encryption and decryption times are comparatively nearer to the previously existing well known encryption algorithms. With proper key management technology it can become one of the efficient cryptographic algorithms used to achieve greater degree of confidentiality and integrity in a simple way.

REFERENCES

[1] Ms. Kruti Sharma and Prof. Kavita R Singh, "Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies, IEEE Computer Society, DOI 10.1109/CSNT.2013.85,2013.

[2] Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, "Parity Cloud Service:A Privacy Protected Personal Data recovery service", 2011 International Joint Conference of IEEE Trust com-11/IEEE ICESS-11/FCST-11.

[3] Kathryn James, "How does Cloud storage work", March 05, 2014.

[4] Disaster Recovery and Business Continuity Planning, Quest Technology Management, "Disaster Recovery Services and Planning Solutions".

[5] "How-cloud-storage-works.html", Tutorials Point, Dec 10, 2012.

[6] Krishna Shankar," How does Cloud storage service work", Tutorials Point, June 5, 2012.

[7] Mohammad Ali Khoshkholghi, Azizol Abdullah, Rohaya Latip, Shamala Subramaniam and Mohamed Othman, "Disaster Recovery in Cloud Computing: A survey", Computer and Information Science, Volume 07, No.4; 2014. ISSN 1913-8989 E-ISSN 1913-8997, Published by Canadian Center of Science and Education.