A Synopsis on

Enhancing Security in Cloud Storage using ECC

Submitted in partial fulfillment of the requirements
of the degree of

Bachelor of Engineering

in

Information Technology

by

Rizwan Khan (15204050)
Tejas Waragade (15204018)

Guide: Prof.Rahul Ambekar

Department of Information Technology
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI
2018-2019

CERTIFICATE

This is to certify that the project Synopsis entitled ***"Enhancing Security in Cloud Storage using ECC"*** Submitted by ***"Rizwan Khan(15204050),Tejas Waragade(15204018)"*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Information Technology.***to the University of Mumbai,is a bonafide work carried out during academic year 2018-2019

(Prof.Rahul Ambekar)
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place: A.P.Shah Institute Of Technology,Thane
Date:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Rizwan Khan(15204050))

_____

(Tejas Waragade(15204018))

Date:

Abstract

Security in cloud computing is an evolving area in todays world. It is subject of concern for Cloud Technology Services.One of the measures which customers can take care of is to encrypt their data before it is stored on the cloud.

Today, the cloud storage is fulfilling the need for more storage space to hold all of your digital data. Cloud storage providers operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them.

The data center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects.Physically, the resource may span across multiple servers.

This work is intended towards providing security service such as confidentiality in the cloud services can use Elliptic Curve Cryptography (ECC) algorithm.

In this paper we are secure saving of our data in the cloud storage in an efficient way which need use less CPU Power and Processing time so we are using Electronic Curve Cryptography (ECC) algorithm for security purpose and for integrity we create and encrypt Meta data using certain algorithm to enhance further security or for confidentiality of data. It is Novelty of our work proof by results.

Introduction

Cloud computing security has become a hot topic in industry and academic research. This will explore data security of cloud in cloud computing by encryption and decryption with elliptic curve cryptography.Elliptic curve cryptography has the advantages over the familiar and generalized RSA in terms of smaller key sizes, lower CPU time and less memory usage.

OVERVIEW

A. DEPLOYMENT CLOUD MODELS

Public cloud:- The cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.

Private cloud:- The cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.

Community cloud:- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.

Hybrid cloud:- the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

B. CLOUD CHARACTERISTICS

On demand service:- Cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.

Ubiquitous network access:-Cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.

Easy use:- The most cloud providers offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.

Business model:- Cloud is a business model because it is pay per use of service or resource.

Location independent resource poling:- The providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

C. CLOUD SOLUTIONS

Infrastructure as a service:- It delivers a platform virtualization environment as a service rather than purchasing servers, software, data centers.

Software as a service:- It is software that is deployed over internet and or is deployed to run behind a firewall in your LAN or PC.

Platform as a service:- This kind of cloud computing provide development environment as a service. You can use the middlemans equipment to develop your own program and deliver it to the users through internet and servers.

Storage as a service:- This is database like services billed on a utility computing basis,e.g., gigabyte per month.

Desktop as a service:- This is the provisioning of the desktop environment either within a browser or as a terminal server.

Figure 1: Cloud Storage

Objectives

One of the chief uses of cloud computing in cloud storage is that data is storage on numerous third party servers, formerly on the steadfast servers uses in antiquated network data storing. When store data, the operator perceives an imitation server that is to say, it seems as if the data is storing in a specific location with particular designation. Conversely, that location does not be existent in actuality. It is just a penname familiar mention virtual space engraved out of the cloud computing. The operators data could be stored on any more than of computers used to produce the cloud computing.

The objectives that we our going to achieve in this paper are as follows:

[1] Sender Login:- In this module, sender can login into the system using username and password authentication and gains the access to the application.

[2] Encryption Module:- In this module, sender enters the message which is to be sent to the receiver and encrypts the message using Elliptic Curve Cryptography.

[3]Receiver Login:- In this module, receiver can login into the system using username and password authentication and gains access to the application.

[4]Decryption Module:-Receiver decrypt the message using his private key.

Literature Review

No.	Title of paper	Author Name	Publication	Methodology	Limitation
1	Providing Security, Integrity and Authentication Using ECC Algorithm in cloud storage.	Ms.Akanksha Bansal & Mr.Arun Agrawal	IEEE(2017)	ECC Algorithm	Expensive for daytime users.
2	Enhancing Security in Cloud Storage using ECC Algorithm.	Mr.Ravi Gharshi & Ms.Suresha	IEEE(2016)	ECC Algorithm	Increases size of encrypted message.
3	Data Security in Cloud Computing with Elliptic Curve Cryptography.	Mr. Veerraju Gampala, Ms.Srilakshmi Inuganti & Satish Muppidi	IEEE(2015)	ECC Algorithm	security issues of cloud computing.

In [1] authors,They have proposed a system, which decrease amount of work of the customer and provide security integrity and authentication in an effectual way. As the data is not physically obtainable to the user the cloud should deliver the user a method to check for integrity..

In [2] authors,They have built the system which is demonstrated the use ECC algorithm for portable devices and applications.

In [3] authors,They have build system which have the concern with data security with Elliptic curve cryptography to provide confidentiality and authentication of data between clouds

Problem Definition

A cloud typically contains a virtualized significant pool of computing resources. The entire process of requesting and receiving resources is typically automated and is completed in minutes.The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service.

However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for the users.
Proposed work is that we do not require to encrypt the whole file, We will encrypt only some bits of every block because we can retain the huge volume of data at client side becomes an overhead to user and thus the client computational overhead is reduced so we are providing the security and integrity using ECC algorithm and we also provide authentication for more security. Our system is efficient in the manner that it usage extra less CPU power and execution time.

Proposed Architecture

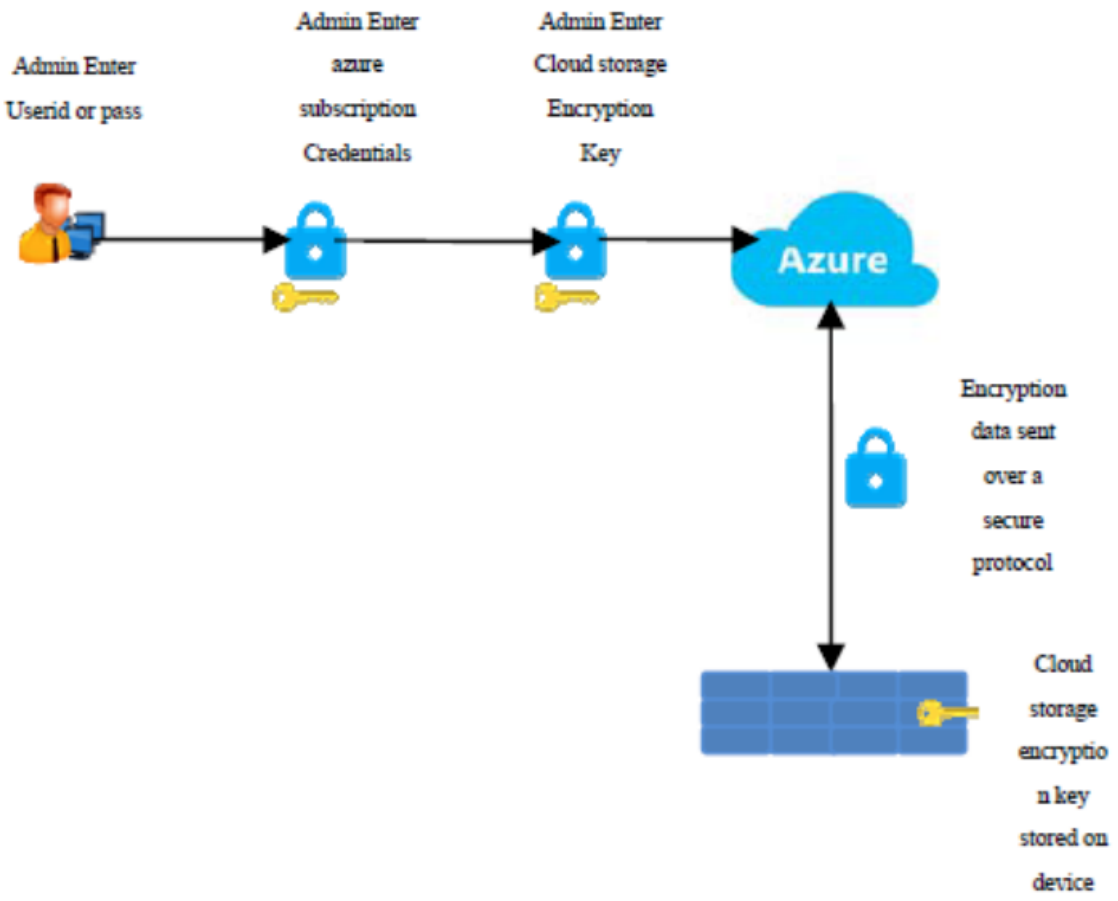

Figure 2: Proposed Architecture

In propose a system,which decrease Amount of work of the customer and provide security integrity and authentication in an effectual way. As the data is not physically obtainable to the user the cloud should deliver the user a method to check for integrity. We delivered a method which gives an evidence of the integrity for the data in the cloud which the client employs to check the accuracy of user data in the cloud. To secure the cloud resources protected the behaviors and storage databases hosted by the Cloud provider Three Security goals of the data comprise points namely:- Confidentiality, Integrity, and Availability (CIA). Data Privacy in the cloud is achieved by Decryption/encryption process. In this proposed work we do not require of encrypted the whole file. We encrypt only some bits of every block because we can

retain the huge volume of data at client side becomes an overhead to user and thus the client computational overhead is reduced so we are providing the security and integrity using ECC algorithm and we also provide authentication for more security. Our system is efficient in the manner that it usage extra less CPU power and execution time.

Summary

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques like RSA, AES, DES, etc.
As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security. After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA. The ECC has many advantages due to its ability to provide the same level of security as RSA yet using shorter keys.
Cloud computing is a model for providing IT facilities in which assets are regained from the internet over web-based applications and tools, sooner than a directly linking to a server. In this paper We save our data in the cloud storage using authentication and also provide security and integrity checking for our data to verify and also use Electronic Curve Cryptography algorithm for security in this way that it use a reduced amount of processing time and CPU Power and also provide efficient method for clients use small device like PDA and Mobile etc.

References

[1] Ms.Akanksha Bansal and Mr.Arun Agrawal, Providing Security, Integrity and Authentication Using ECC Algorithm in cloud storage, IEEE-2017

[2] Mr.Ravi Gharshi and Ms.Suresha, Enhancing Security in Cloud Storage using ECC Algorithm, IEEE-2016

[3] Mr.Veerraju Gampala, Ms.Srilakshmi Inuganti and Satish Muppidi, Data Security in Cloud Computing with Elliptic Curve Cryptography.

[4] Pachipala Yellamma, C h a lla Narasimham and Velagapudi sreenivas Data Security in Cloud using RSA 4th International Conf. of ICCCNT, IEEE-2013

[5] Ali Siam, Hatem Abdelkader and Mustafa M. Abd Elnaby Enhanced Data Security Model for Cloud Computing Platform International Journal of Scientific Research in Science, Engineering and Technology ijsrset.com , Research Gate-2015