Providing Security ,Integrity and Authentication Using ECC Algorithm in cloud storage

Akanksha Bansal
Computer Science & Engineering
Institute of technology & Management
Gwalior, India
akankshabansal10@gmail.com

Arun Agrawal
Computer Science & Engineering
Institute of technology & Management
Gwalior, India
development_arun@rediffmail.com

Abstract— **Cloud computing is a sort of computing that is contingent on distribution computing resources preceding having innate servers or specific plans to knob applications. In the cloud computing Cloud storage avoids the need to buy storage and also allows user to access broad range of application and resources immediately, which are hosted by others. But difficulty is our data security is not grauntaneed in cloud storage because that it prevents intruders from accessing our private data and also it prevents modification of data by unauthorized users so providing security integrity and authentication. 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.**

Keywords—Confidentiality, Integrity, Authentication, Cloud Storage, ECC, SLA

I. INTRODUCTION

Cloud computing is a well-defined by the National Institute of Standards and Technology (NIST) It is a computing facilities provision ideal for where simulated resources are delivered as a facility above the Internet and animatedly scalable. Cloud is a ideal for allowing useful , on-demand network accessed to a communal pond of the configurable cloud resources (for example applications, storage, services and servers) that can be quickly delivered and unconfined with nominal managing exertion or facility supplier contact". Cloud computing well-defined and reference design are definite in NIST publication. NIST has proposed an allusion cloud computing classic composed of four deployment models and three service models.

There are three Service models are Software as a Service (PaaS), Platformas a Service (IaaS) and Infrastructure as a Service (SaaS) There are four deployment models which are private cloud, community cloud, public cloud and hybrid cloud. Though, The ISO ruling has seven diverse cloud service categories, addition to the earlier service models:, computing as a service (CompaaS), Network as a service (NaaS), and data storage as a service (DSaaS) There is rising interest in the cloud from cloud Service Providers and Consumers.

As of the standpoint of the data confidence protection, which has continuously been a significant feature of the quality of service (QoS), the determination of the cloud data security cannot be directly accepted owed to the users' damage control of data below Cloud. Subsequently, confirmation of the correctness data storing in the cloud computing must be coxswained deprived of overt familiarity of the entirely data. As several kinds of the data for every user storing in the cloud computing and the plea of long term never-ending guarantee of their data security, the effort of verifying precision of the data storage in the cloud becomes entirely the further challenging.

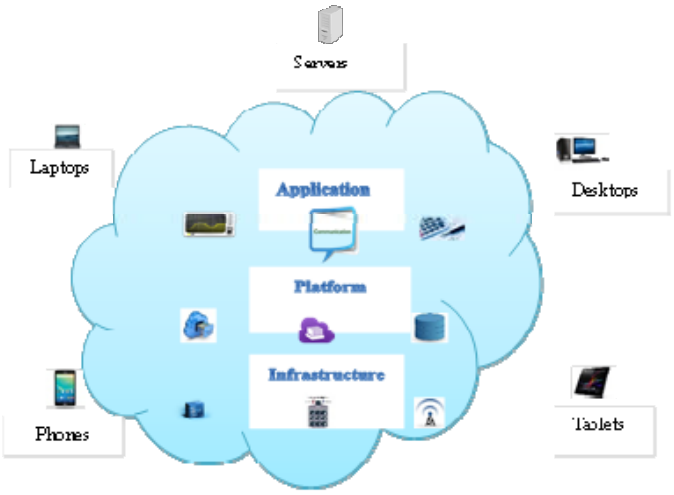

Fig1. Cloud computing Architecture

As single of the central facilities of the cloud, cloud storing has expanded huge development in modern years and has been extensively deliberated as a largely storage method in the upcoming. Data is storing in the cloud computing have several benefits for instance redeemable hardware price, simplifying administration and humanizing storage

978-1-4673-8855-9/17/$31.00 ©2017 IEEE

consistency. However, the steadiness and safety of the data storing in the cloud computing continue main anxieties, and Are flattering the vital issues obstructive extra development of the cloud computing storage. On the one hand, employers concern about the privacy of their data which storage in the cloud computing can't be assurance.

II. RELATED WORK

Tawalbeh et al. In this paper, we tend to proposed associate effectual confidentiality-based cloud storage framework that enhance the interval and guarantees integrity and confidentiality through knowledge taxonomy and apply SHA, AES and TLS founded the sort of classified data. The potency of our planned framework has been shown through conducting simulations. and applied AES, SHA and TLS supported the sort of classified data. The potency of our planned framework has been shown done conducting imitations. In this paper, we tend to area unit familiarizing a cloud framework that categorizes the information based on their significance. In other words, a lot of important data are going to be encrypted with extra secure encryption algorithm and larger key sizes, whereas less important data may even not be encrypt.

Yellamma et al. Clouds proposal on-demand accessed to the computing utilities, a concept of infinite computing capitals, and maintained for on-demand scale down, scale out and proportion. Applications while not installed and access their private files at some computer with internet access. The Rivest Shamir algorithmic rule (RSA) delivers the tall safety in higher potential encryption technique; the cloud computing are used to retain the condition of the protection and relinquishment the case. In this paper we have a tendency to ar that specialize in issues linking to the cloud data storage ways that and safety within the virtual atmosphere. We have a tendency to projected how for provide data storage and safety within the cloud computing via public key cryptosystem RSA. Additional, defines the protection facilities contains decryption and encryption.

Choubey et al. Cloud computing is a network based technology as security problems like confidentiality, privacy and data security etc. In this study, we observed that most of the Privacy Preserving and security solutions proposed by the authors have complex adaptable behavior in its working environment. Hence we need a well-organized privacy preserving & security model (Encryption based) which could be easily adopted in current working environment of cloud. Our future work will focus on proposing a fast encryption solution that should be adjusted in each part of the cloud There are some solutions proposed, to resolution these issues, based on some solutions proposed, to resolution these issues, based on encryption techniques. The chief contribution of this paper is to perform a study of different solutions to provide data privacy and security in existing cloud computing scenario.

Kumar et al. In this paper we have operated to modify the client in receiving a proof of the integrity of the data that he must store within the cloud storage servers with unadorned min efforts and prices. We tend to conjointly scale back the scale of the proof of data integrity in order to decrease the network bandwidth ingesting. Since the data is physically not available to the user the cloud computing should deliver a way for the user to ascertain if the integrity of his data is compromised or preserved. In this paper we tend to deliver a system which give proof of the integrity within the cloud that the consumer will employment to checked the accuracy of the data in the cloud computing. This proof will be organized upon by each the cloud and also the consumer and may be unified within the SLA (Service level agreement). This process to make sure that the storing at the consumer side is nominal which is able to be valuable for skinny clients.

Shanmugakani et al. In our proposed system, we tend to tested the issue of data protection within the cloud data storage within the cloud computing. We tend to uses the express integrity verification method, which decrease the data wedge verification, the number of computation on the server and customer and also no necessity to uses Third Party Authority (TPA). Our scheme encounters the goals of data integrity and security verification and since of the easy interactions; our method is executed capably and quietly. In this paper, we tend to projected a unique methodology to achieved integrity objectives and that we discover a way to ensure the integrity and accuracy of the data storage within the cloud computing. The distinctive feature of this method is find out that data portion is changed or attacked by the malevolent user

III. BASIC CONCEPT OF CLOUD STORAGE

One of the chief uses of cloud computing in cloud storage. Using the cloud storage, data is storage on numerous third party servers, formerly on the steadfast server's 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 operator's data could be stored on any more than of computers used to produce the cloud computing.

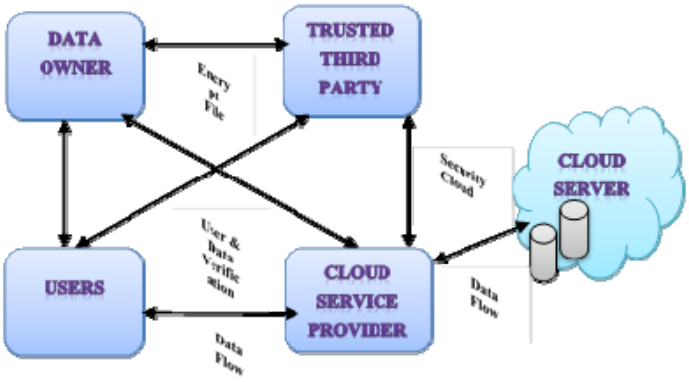

Fig2.Cloud Data Storage

Advantages

• In the cloud storage evades the requirement to purchase storing kit.

•We are using then we have to just pay for the quantity of storage.

• The permits user to accessed wide range of resources instantly and applications, which are hosted by others in the cloud storage.

Disadvantages

• Jobless data it clues to be hacked by illegitimate users

• It is expensive for daytime users

• In the cloud storage security is not assurance entirely for our data.

IV. PROPOSED WORK

In this paper we are going 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.

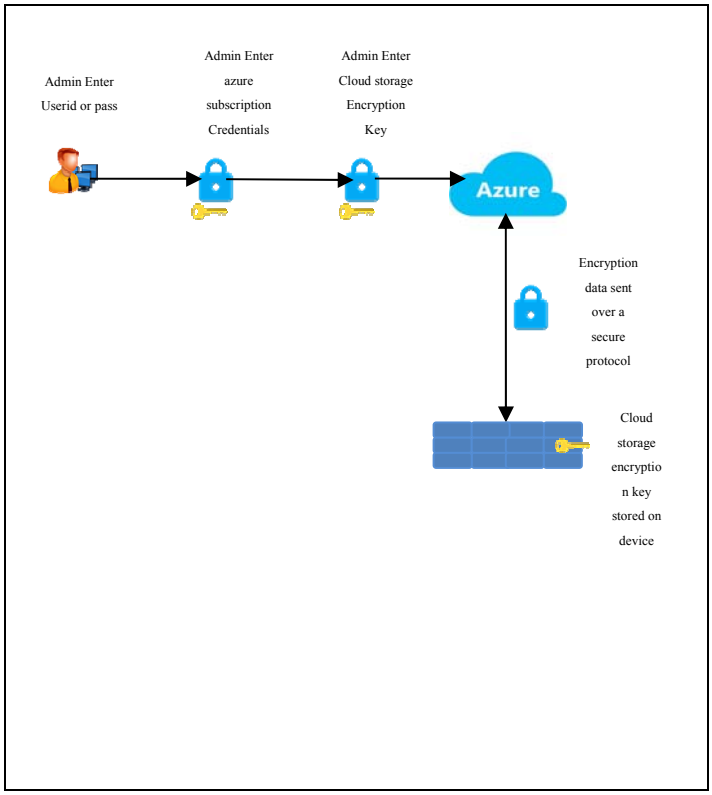

Fig3: Model of encryption & Decryption in cloud storage

- The user is single who wants to access the cloud storing for storage the data.
- For safe access every user is give a unique key done which he can access his explanation and acquire the welfares of the cloud computing storage.
- The data earlier storage it is encrypt via ECC algorithm. In cloud computing usage 56 bits, vacter size 64 bits, contain less than capacity, execution time is Equals to ECC and encrypt ion and decrypt ion same key is used and also image matching for authentication
- Then encrypted file is saved in the library.
- It is verify the integrity the user appeal the Meta data.
- The user compared to the Meta data and get whether the data is accurate or changed.
- If the file has been changed it is specified to the users

A. Providing Security using ECC as compared to RSA

The data that the user stores in the cloud storage should be secure so as to it prevents interlopers from accessed our private data [4]. To provide security

using ECC is a secure and extra effectual encryption algorithm than Rivest-Shamir-Algorithm (RSA) as it uses negligible key sizes for equivalent level of security as compared to RSA. For e.g. a 256-bit ECC public key provides differentiate security to a 3072-bit RSA public key. The goal of this work is given by insight into the use of ECC algorithm for data encryption before uploading the data on to the cloud. ECC increases the size of the encrypted message significantly more than RSA encryption and it is mathematically extra subtle than RSA. In my base paper using RSA for security. So we are showing ECC is much better than RSA.

Elliptical curve cryptography (ECC) is a public key encryption technique founded on elliptic curve theory that can be used to make faster, lesser, and more effectual cryptographic keys. ECC generates keys through the possessions of the elliptic curve equation instead of the traditional process of generation as the product of very large prime numbers. Since ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile application.

B. Integrity checking using Meta data

When the user want to store data in cloud storage then uploading a file it processor and user generate the Meta data and Entire Meta data choose from every data block are encrypt with ECC algorithm to extra more security. The Meta data created and encrypted via the exceeding techniques are added at the back of the file. The encrypt file with Meta data is archived in the cloud. The verifier uses the Meta data to verify the integrity of the user data. We do the opposite process of encryption and decryption and see if the Meta data that was added back of the file is modified or correct. If file is not modified and therefore we get an evidence of retrievability.

V. RESULT

Fig4: Home Form (Welcome to secure cloud storage)

Fig5: Register Form (Register successfully)

Fig6: Login Form (User id to login)

Fig7: Uploading a file (check thumb)

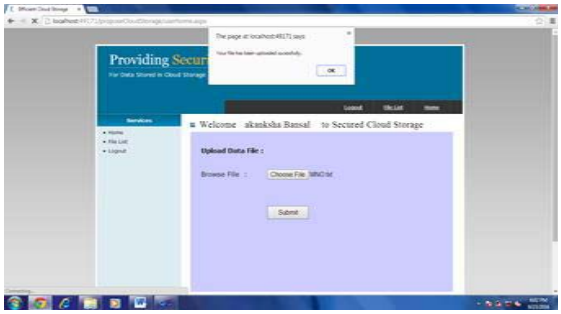

Fig8: Upload data file form (file uploaded successfully)

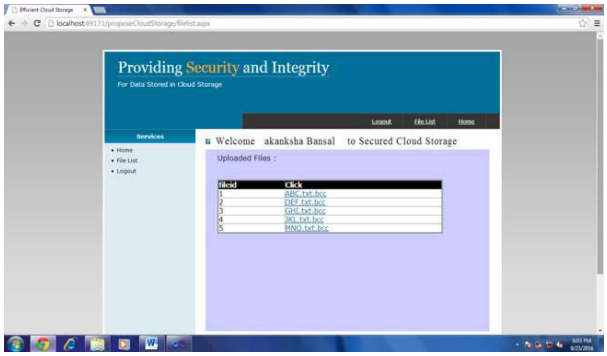

Fig9: File list form (Uploaded files in file list

VI. CONCLUSION

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] 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

[2] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing" IEEE-2009

[3] Yongkang Fu1 and Bin Sun "A Scheme of Data Confidentiality and Fault-Tolerance in cloud storage" IEEE CCIS-2012

[4] Loai Tawalbeh and Yaser Jararweh "Secure and Efficient Cloud Computing Framework" International Conference on Cloud and Autonomic Computing, Research Gate-2015, DOI: 10.1109/ICCAC.2015.45

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

[6] Siddharth Dutt Choubey and Mohit Kumar Namdeo "Study of Data Security and Privacy Preserving Solutions in Cloud Computing" International Conference on Green Computing and Internet of Things (ICGCloT) , IEEE-2015

[7] Sravan Kumar R and Ashutosh Saxena "Data Integrity Proofs in Cloud Storage"

[8] N. Shanmugakani and R. Chinnaa "An Explicit Integrity Verification Scheme for Cloud Distributed Systems" 9th International Conference on Intelligent Systems and Control (ISCO), IEEE-2015

[9] Arjun Kumar 1 , Byung Gook Lee2, HoonJae Lee2 "Secure Storage and Access of Data in Cloud Computing" IEEE ICTC-2012

[10] Mr.Chandrashekhar S. Pawar ,Mr.Pankaj R. Patil "Providing Security and Integrity for Data Stored in Cloud Storage" ICICES2014 - S.A. Engineering College, Chennai, Tamil Nadu, India , IEEE 2014

BIOGRAPHY

Akanksha Bansal was born in 21th August 1992. She received the Bachelorof Engineering in Computer Science & Engineering from Shriram College of Engineering & Management (Banmour). Gwalior, India in 2014, and she is presently pursuing M.tech in Computer Science & Engineering from ITM Universe, Gwalior, India. Her main area of research interest as Data mining, cloud computing & cloud databases.

Arun Agrawal is currently working as Assistant Professor in Department of Computer Science & Engineering of Institute of Technology & Management, Gwalior. His research areas are Vehicular Adhoc Networks, Embedded System, Digital Image Processing.