International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

Enhance Data Security in Cloud Computing

G. Shaheen Firdous[1], C. Vani[2], D. Kavya Sree[3], G. Mounika[4]
[1]Guide Assistant Professor, [2,3,4]U.G. Scholar
[1,2,3,4]Computer Science And Engineering
[1,2,3,4,] Ravindra College of Engineering For Women
Email :[1]shaheencse@recw.ac.in, [2]vaanichintamanu@gmail.com,
[3] kavyasree1513@gmail.com, [4]mounika.g2018@gmail.com

ABSTRACT

Cloud computing is the adept innovation for the ten years. It permits clients to store a lot of data in cloud capacity and use it as and when expected, from any region of the planet, by means of any terminal hardware. Since cloud computing lays on the web, security issues like privacy, data security, secrecy, and verification are experienced. To dispose of something very similar, different encryption algorithms and instruments are utilized. Numerous scientists pick the best they found and use it in various mixes to give security to the data in the cloud. In comparative terms, we have chosen to utilize different confirmation procedures and basic trade algorithms mixed with an encryption algorithm. This mix is alluded to as a "Three way component" since it guarantees each of the three insurance plans of validation, data security, and confirmation at the same time.

In this paper, we propose utilizing a computerized signature and Diffie Hellman key trade mixed with (AES) Advanced Encryption Standard encryption algorithm to safeguard the secrecy of data put away in the cloud. Regardless of whether the key in the transmission is hacked, the Diffie Hellman key trade office renders it pointless since the key on the way is of no utilization without the client's confidential key, which is restricted exclusively to the genuine client. This proposed design of a three-way component makes it extreme for programmers to break the security framework, subsequently safeguarding data put away in the cloud.

Keywords :Cloud computing; Security; Privacy; Data security; Cryptography

INTRODUCTION

Cloud computing essentially implies Internet computing. Commonly the web is viewed as an assortment of clouds; in this way, the word cloud computing can be characterized as using the web to give innovation-empowered administrations to individuals and organizations[5]. Cloud computing is a new utility of the 100 years, which many endeavors need to consolidate to work on their approach to working. It infers sharing of computing assets to deal with applications. Cloud computing offers decreased capital consumption, functional dangers, intricacy, and upkeep, and expanded versatility while offering types of assistance at various reflection levels, namely software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS)[6]. It is utilized in shopper-situated applications, for example, monetary portfolios conveying customized data or power vivid PC games. It is compensation as examine sort of administration, subsequently has become highly famous in significantly less time. Since cloud computing is a utility accessible on the net, so different

issues like client privacy, data robbery and spillage, overhang dropping, unauthenticated access, and other programmers' assaults are raised.
These inexplicable security issues of confirmation, privacy, data insurance, and data check are primary obstructions to the inescapable reception of cloud computing. Subsequently, to get an overpowered acknowledgment to cloud computing in money, market, and industry, we have proposed a protected design for it. Under the previously mentioned title, I am consolidating three security control components- confirmation, Encryption, and data check method- into a solitary independent framework. Thus it is a three different ways security plot wherein computerized signature gives verification, encryption algorithm gives meeting encryption key and is utilized for encoding client data document too, which is to be saved in the cloud and conclusion confided in computing to confirm uprightness of client data.

PROBLEM STATEMENT

With cloud computing, associations can utilize administrations, and data is put away in any area unchangeable as far as they might be concerned. This office brought up the different security issues like privacy, classification, honesty, and so forth and requested a confided-in computing climate wherein data secrecy can be kept up with. To prompt confidence in the computing, there is a need for a framework that performs validation, checks,s and encoded data move, subsequently keeping up with data privacy.

Table 1 : Types of Attacks

Name of Attack	Description
Tampering	An attacker may alter information either stored in local files, database or is sent over public network.
Eavesdropping Information Disclosure	This type of attack occurs when attacker gains access in the data path and gains access to monitor and read the messages.
Repudiation	Sender tries to repudiate, or refute the validity of a statement or contract which is sent by him/her.
Elevation of Privileges	An attacker may access unauthorized to information and resources
Man-in-the-Middle Attack	This type of attack occurs when an attacks infiltrates the communication channel in order to monitor the communication and modify the messages for malicious purposes
Replay Attack	A replay attack is defined as when an attacker or originator sends a valid data with intention to use it maliciously or fraudulently.
Identity Spoofing	Identity spoofing occurs when an attacker impersonates the users as the originator of the message in order to gain access on a network.
Differential Analysis Threat	When new versions are released, a differential analysis of the new and old version would indicate where differences in the code exist
Viruses and Worms	Viruses and worms are very common and well known attacks. These are piece of code that decrease the performance of hardware and application even these malicious codes corrupts files on local file system

LITERATURE REVIEW

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

According to Uma Somani, Kanika Lakhani, and Manish Mundra [1]: In Cloud computing, we have a problem with the security of data, records framework, reinforcements, and network traffic, have security. They have proposed the idea of a computerized signature with an RSA algorithm to scramble the data while moving it over the organization. This procedure takes care of the double problem of verification and security. The strength of their work is the system proposed to address security and privacy issue.

Volker Fusenig and Ayush Sharma [2] state another methodology called cloud organizing, which adds functionalities to cloud computing and empowers dynamic and adaptable situations of virtual assets crossing supplier borders. This permits different advancements, e.g., decreasing inertness or organization load. This paper presents a security design that empowers a client of cloud systems administration to characterize security prerequisites and implement them in the cloud organizing framework.

According to Deyan Chen and Hong Zhao [3], from the shoppers' viewpoint, cloud computing security concerns are unique data security and privacy insurance issues that stay the essential inhibitor for the reception of cloud computing administrations. However, they gave a brief all over the investigation on data security and privacy insurance issues related to cloud computing across all phases of the data life cycle. Then, at that point, they proposed to safeguard data utilizing different plans and arrangements like air vat and so on. This framework can forestall privacy spillage without approval in the Map-Reduce computing process.

The shortcoming is that it is simply a hypothesis challenged. Each cloud supplier takes care of this problem by scrambling the data using encryption algorithms. Consequently, their paper explores the fundamental problem of cloud computing data security. They introduced the data security model of cloud computing because of the investigation of cloud engineering. They programmed to upgrade work in a data security model for cloud computing. At long last, they applied this product in the Amazon EC2 Micro occurrence for the assessment process.

G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom [9]: proposed to create RSA Public keys and Private Keys for public and confidential admittance to defeat the problem of data security. Declaration Binary document is utilized inside control hub setup record to ensure cloud data stream safely. The control hub sends data through the Secure Socket Layer after authentication enactment.

At extended last AES algorithm is utilized for encryption. This particular mix makes this arrangement best to forestall various sorts of assaults. The strength of their work areas of strength for is security against other assaults. On the off chance that a client is an endeavor to login dishonestly ordinarily, the framework consequently eases back the help and briefly stops the record administration for the specific client

PROPOSED SYSTEM

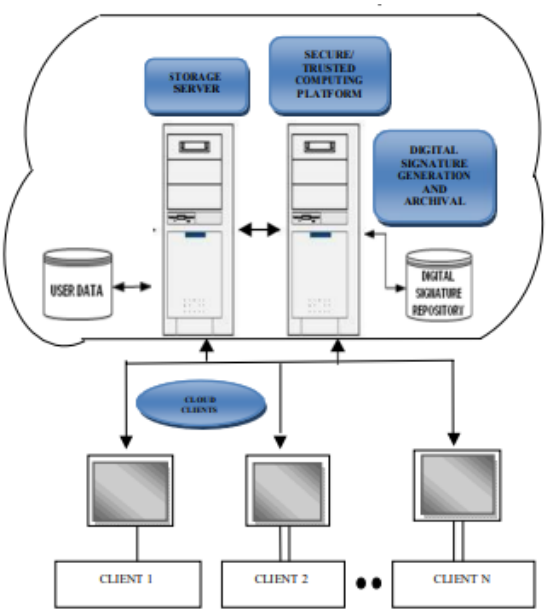

Figure 1. Proposed Architecture

In our proposed engineering, we are utilizing three different ways security plots. Diffie Hellman algorithm, first and foremost, is used to produce keys for essential trade steps. Then computerized mark is used for validation, and from there on, the AES encryption algorithm is used to encode or unscramble the client's data document. This is carried out to give believed STORAGE SERVER SECURE/TRUSTED COMPUTING PLATFORM DIGITAL SIGNATURE GENERATION AND ARCHIVAL CLOUD CLIENTS CLIENT 1 CLIENT 2 CLIENT N computing climate to stay away from data adjustment at the server end. For a similar explanation, two separate servers are kept, one for the encryption process known as the (trusted) computing stage and one more known as the capacity server for putting away client data documents.

When a client needs to transfer a record to the cloud server, the first key is traded utilizing Diffie Hellman key trade at the hour of login, and then, at that point, the client is verified using a computerized signature. At long last client's data document is encoded utilizing AES, and at that time, it is transferred to another (cloud) Storage server. When the client needs the same record, it is to be downloaded from the cloud server. For that reason, when the client logs in, the first encryption keys are traded, the paper to be downloaded is chosen, and verification happens to utilize a computerized signature. At that point, AES is used to unscramble the saved document, and the client can get to the document

A. Execution Steps:
1. Sign up
2. Login from TCP Key Exchange – Diffie Hellman Digital Signature –SHA-I
3. Uploading / Downloading Data Encryption- AES
4. Data is stored / retrieved from Storage server
5. Logout.

B. Hardware specification: The system running the application should have following minimum requirements:

1. Pentium Core.
2. RAM Size 128mb.
3. Processor 1.2GHz.

C. Software specification:
The system running the application must have the following:
1. Supporting OS: Windows XP, VISTA, LINUX: Red Hat, Ubuntu, Fedora.
2. Java Development Kit - jdk1.6.0_02.
3. Java Runtime Environment -jre1.6.0_06.
4. Web Browser like Google chrome with Java Plug-in installed.

5. Wireless connectivity driver. D. Technology Specific Tools used In this work we use following technology tools:

1. Java Development Kit - jdk1.6.0_02.
2. Java Runtime Environment - jre1.6.0_06.
3. Java.awt package for layout of the applet.
4. Java.net package for connection settings and message passing.
5. Netbeans
6. Java Web Start.
7. SOAP.
8. Glassfish Server.
9. Socket Optionsinterface of methods to get/setsocket options

CONCLUSION

As of now cloud computing is at the beginning stage. As anventure understands its advantages over a period, utilization of cloudis supposed to increment perpetually. Cloud would work withconveyance of increasingly more practical it administrations. Cloudcomputing is a quickly developing model with new capabilities, developments and updates being consistently reportedfurthermore, must be used to acquire most extreme yield. CloudComputing has the capability of being the leader indeveloping of a got and financially suitable IT solution. The cloud needs to target little and medium sizeorganizations for relocating their organizations to the cloudwhich would diminish costs and would give them the opportunity to get to innovations and applications which wereprior past the scope of associations

REFERENCE

[1] Uma Somani, Kanika Lakhani, Manish Mundra “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
[2] Volker Fusenig and Ayush Sharma “Security Architecture for Cloud Networking” 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.
[3] Deyan Chen and Hong Zhao “Data Security and Privacy Protection Issues in Cloud Computing” 2012 IEEE International Conference on Computer Science and Electronics Engineering.

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

[4] Zhang Xin , Lai Song-qing and Liu Nai-wen “Research on Cloud Computing Data Security Model Based on Multidimension” 2012 IEEE International symposium on information Technology in medicine and education.
[5] Farhan Bashir Shaikh and SajjadHaider “Security Threats in Cloud Computing” 2011 IEEE 6 th international conference on Internet Technology and secured transactions, 11-14 December 2011, Abu Dhabi United States of Arab Emirates.
[6] Balachandra Reddy Kandukuri, RamacrishnaPaturiV, AtanuRakshi, “Cloud Security Issues” 2009 IEEE International Conference on Services Computing.
[7] Ayesha Malik and Muhammad MohsinNazir ”Security Framework for Cloud Computing Environment: A Review” in Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 3, March 2012.
[8] Sherif el-etriby ,Emanm.Mohamed and Hatem s. Abdelkader published “Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing “ in the third international conference on communications and information technology ICCIT 2012. [9] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom “Implementation of Data Security in Cloud Computing” International Journal of P2P Network Trends and Technology- Volume1 Issue1- 2011 .
[10] Mohamed Al Morsy, John Grundy and Ingo Müller “An Analysis of The Cloud Computing Security Problem” Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia,30thNov2010