Journal of Engineering Sciences
Vol 13, Issue 04, APRIL/2022
ISSN NO:0377-9254

Using public key cryptography and digital signatures to ensure data security in cloud computing

B. RAJA KOTI[1] , S. NAGA VARSHINI[2], KESAPRAGADA SAI MOHAN[3], NEELAPU YOGESH VENKATESH REDDY[4], GUDIVADA SAI ROHITH[5]

#1,Assistant Professor, Department of CSE, GITAM (deemed to be University), GITAM Deemed to be University Rudraram, Hyderabad, Telangana, India

#2,#3,#4,#5 Student, Department of CSE, GITAM (deemed to be University), GITAM Deemed to be University Rudraram, Hyderabad, Telangana, India

ABSTRACT_

Cloud computing is the apt science for the decade. It approves consumer to save giant quantity of records in cloud storage and use as and when required, from any section of the world, by any terminal equipment. Since cloud computing is relaxation on internet, safety problems like privacy, information security, confidentiality, and authentication are encountered. In order to get rid of the same, a range of encryption algorithms and mechanisms are used. Many researchers pick out the nice they discovered and use it in one of a kind aggregate to supply safety to the statistics in cloud. On the comparable terms, we have chosen to make use of a mixture of authentication method and key alternate algorithm blended with an encryption algorithm. This aggregate is referred to as "Three-way mechanism" due to the fact it ensures all the three-protection scheme of authentication, statistics protection and verification, at the equal time. In this paper, we have proposed to make use of digital signature and Diffie Hellman key change blended with (AES) Advanced Encryption Standard encryption algorithm to shield confidentiality of facts saved in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key change render it useless, considering the fact that key in transit is of no use except user's non-public key, which is restrained solely to the reliable user. This proposed structure of three-way mechanism makes it difficult for hackers to crack the safety system, thereby defending facts saved in cloud.

1.INTRODUCTION

Cloud computing is where the data is processed and stored using internet; so, the word cloud computing can be defined as using the internet to deliver technology driven services to organizations and

people. Cloud computing is new utility of the century, which many companies and organizations wants to implement in order to improve their way of working. This means sharing computer resources to process the applications. Cloud computing requires minimal capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). It is used in consumer-focused applications such as financial portfolios delivering personalized information, or power immersive computer games. It is a pay per use kind of service; hence it gained more popularity in less time. Since cloud computing is a service available on net, so various issues like user privacy, data theft and leakage, eaves dropping, unauthenticated access and various hackers' attacksare raised.

2.LITERATURE SURVEY

2.1 Implementing Digital Signature with RSA Encryption Algorithm toEnhance the Data Security of Cloud in Cloud Computing

AUTHORS: Uma Somani, Kanika Lakhani, Manish Mundra

ABSTRACT: The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computingis the Concept Implemented to decipher the Daily Computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.

2.2 Security Architecture for Cloud Networking AUTHORS: Volker Fusenig and Ayush Sharma

ABSTRACT: Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS),

Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). A new approach called cloud networking adds networking functionalities to cloud computing and enables dynamic and flexible placement of virtual resources crossing provider borders. This allows various kindsof optimization, e.g., reducing latency or network load. However, this approach introduces new security challenges. This paper presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in the cloud networking infrastructure.

2.3 Data Security and Privacy Protection Issues in Cloud Computing

AUTHORS: Deyan Chen and Hong Zhao

ABSTRACT: It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud. The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing acrossall stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.

2.4 Research on Cloud Computing

AUTHORS: Zhang Xin , Lai Song-qing and Liu Nai-wen

ABSTRACT: Cloud computing is considered to be the next generation of information technology framework. It is the next generation computing platforms that can provide dynamic resource pools, virtualization and high availability. The new character brings a lot of new security challenges which have not been taken into account completely in the current cloud computing system. As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. In this article, the cloud computing technology architecture and the cloud computing data security features are the first to be studied and considered, then the cloud computing data security model is raised. At last, the realization of data security model has been researched. The model adopts a

multi-dimension architecture of three - layers defense. First of all, user authentication is required to ensure that user data cannot be tampered. Users who pass the authentication can get relative operation on the user data, such as addition, modification, deletion. If the unauthorized user uses illegal means to deceive the authentication system, the file entered the system encrypt and privacy defense levels. In this layer, user data is encrypted. If key has been got by the intruder. The user data cannot be got valid information even it is obtained through function of privacy protection. It is very important for commercial users of the cloud computing to protect their business secrets. The last is the file quick regeneration layer, user data can get maximum regeneration even it is damaged through rapid regeneration algorithm in this layer. Each layer accomplishes its own job and combines with others to ensure data security in the cloud computing.

3.PROPOSED SYSTEM

We use a three-way protection strategy in our proposed architecture. To begin with, the Diffie Hellman algorithm is employed to create keys for the key exchange stage. Then, for authentication, a digital signature is utilised, and the AES encryption method is used to encrypt or decode the user's data file. All of this is done to establish a trusted computing environment and to prevent data alteration at the server end. For the same reason, two different servers are maintained, one for the encryption process known as (trusted) computing platform and another for storing user data files known as storage server. When a user wants to upload a file to a cloud server, the key is exchanged using Diffie Hellman key exchange upon login, and the client is authenticated using a digital signature. Finally, the user's data file is encrypted with AES before being uploaded to another (cloud) storage server. When a client requires the same file, it must now be downloaded from the cloud server. When a user logs in, encryption keys are exchanged first, then the file to be downloaded is selected, authentication is performed using a digital signature, then AES is used to decrypt the saved file, after which the client can access the file.

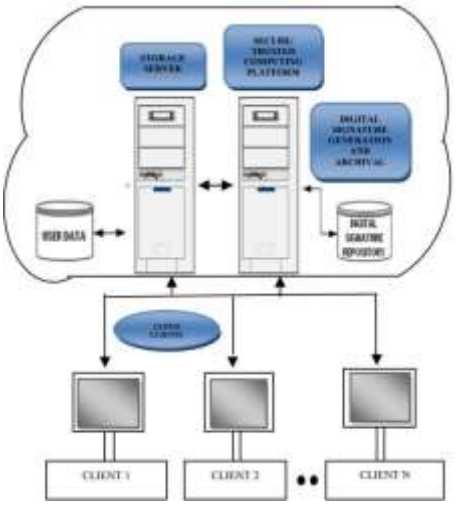

Fig 1:Architecture

3.1 IMPLEMENTAION

To begin the key exchange process, the Diffie Hellman algorithm is utilized to generate keys. The AES encryption algorithm is then used to encrypt or decode the user's data file after which a digital signature is utilized for authentication. All of this is done in order to give a reliable service. To begin the key exchange process, the Diffie Hellman algorithm is utilized to generate keys. The AES encryption algorithm is then used to encrypt or decode the user's data file after which a digital signature is utilized for authentication. All of this is done in order to provide trust.

3.1.1 ALGORITHM:

The Diffie-Hellman algorithm is used to create a shared secret that can be used for secret communications while exchanging data over a public network. The elliptic curve is used to generate points and the secretkey is obtained using the parameters. To simplify practical implementation of the algorithm, we will consider only 4 variables, one prime number P and G (a primitive root of P) and two private values a and b. P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Journal of Engineering Sciences
Vol 13, Issue 04, APRIL/2022
ISSN NO:0377-9254

4.RESULTS AND DISCUSSION

Fig 2:Next, we have to authenticate signature, Then server will authenticate the user

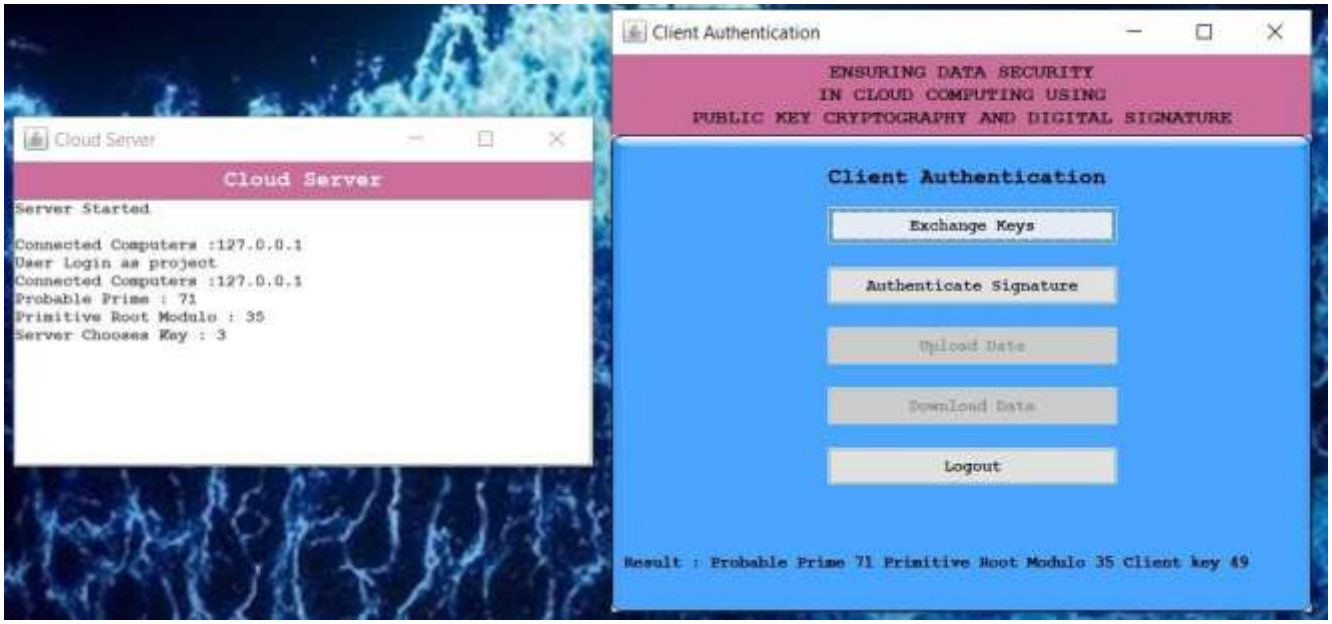

Fig 3:If the authentication is successful, we will get the option to upload and download data

Journal of Engineering Sciences
Vol 13, Issue 04, APRIL/2022
ISSN NO:0377-9254

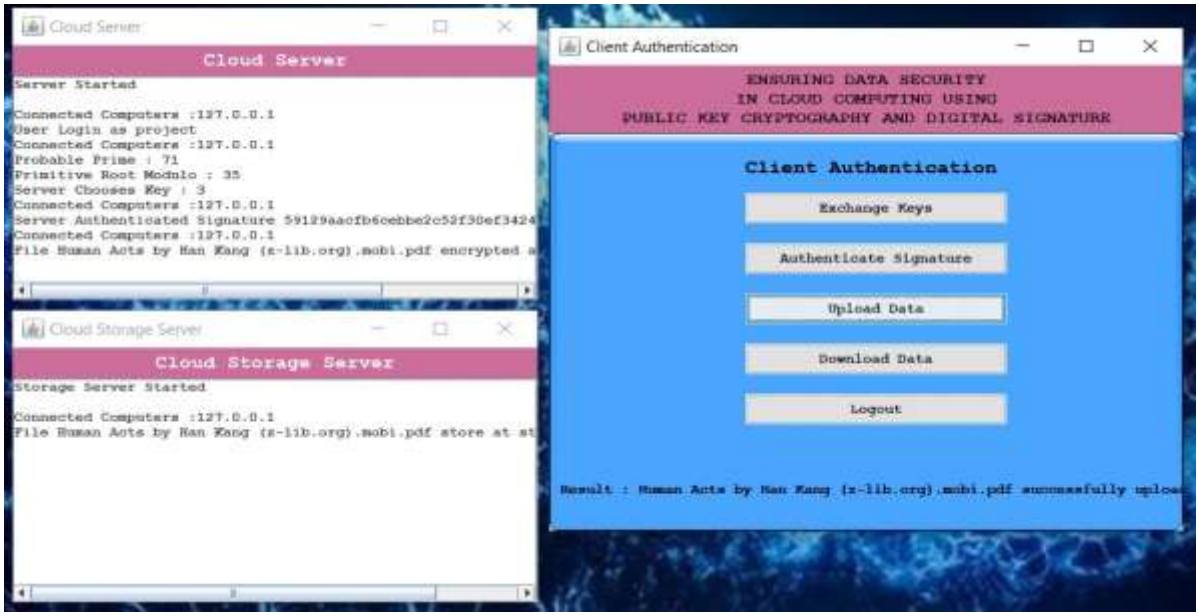

Fig 4:While the data is getting uploaded it will be in ecrypted form and it is done with the help of AESalgorithm

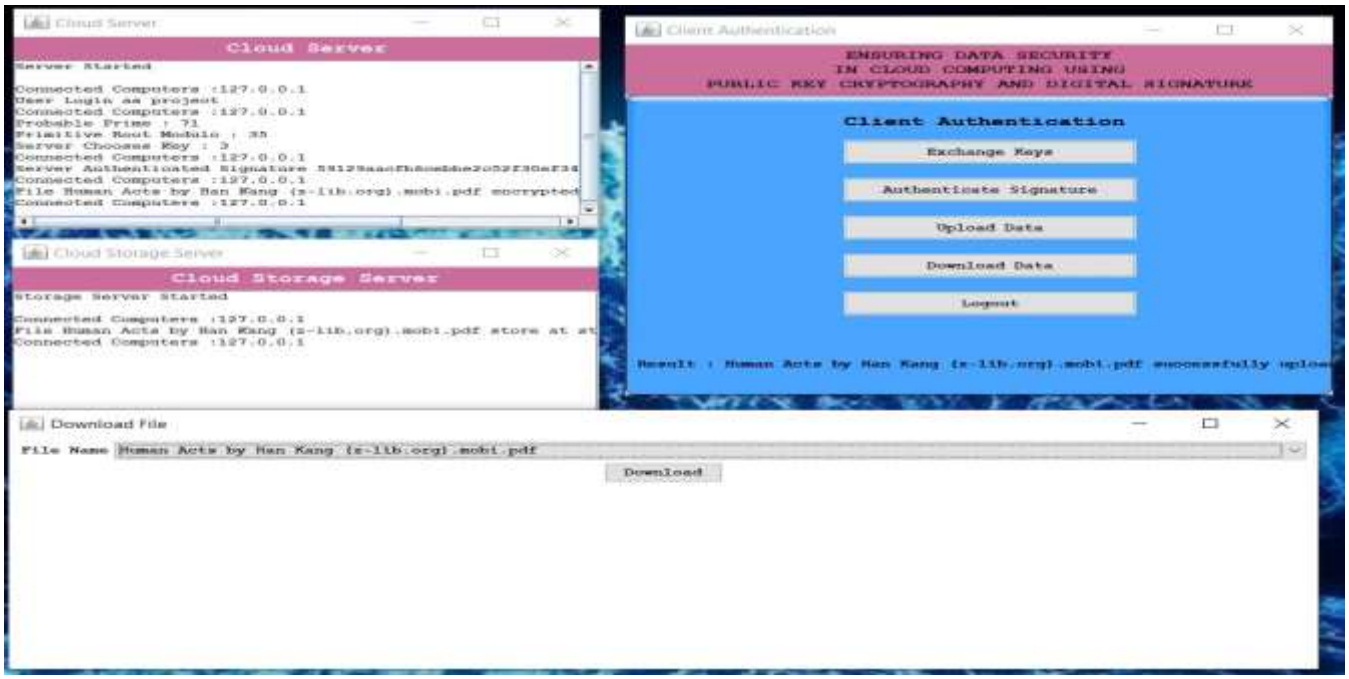

Fig 5:After downloading the data it will be saved into major project directory

Journal of Engineering Sciences
Vol 13, Issue 04, APRIL/2022
ISSN NO:0377-9254

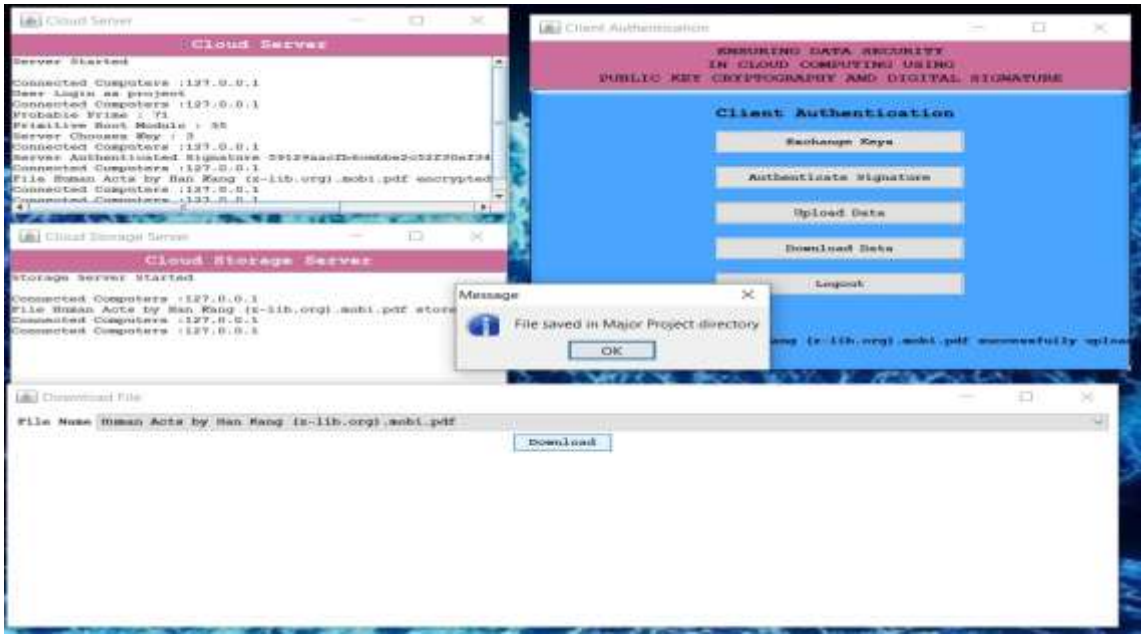

Fig 6:The file saved in the Major Project directory will open.

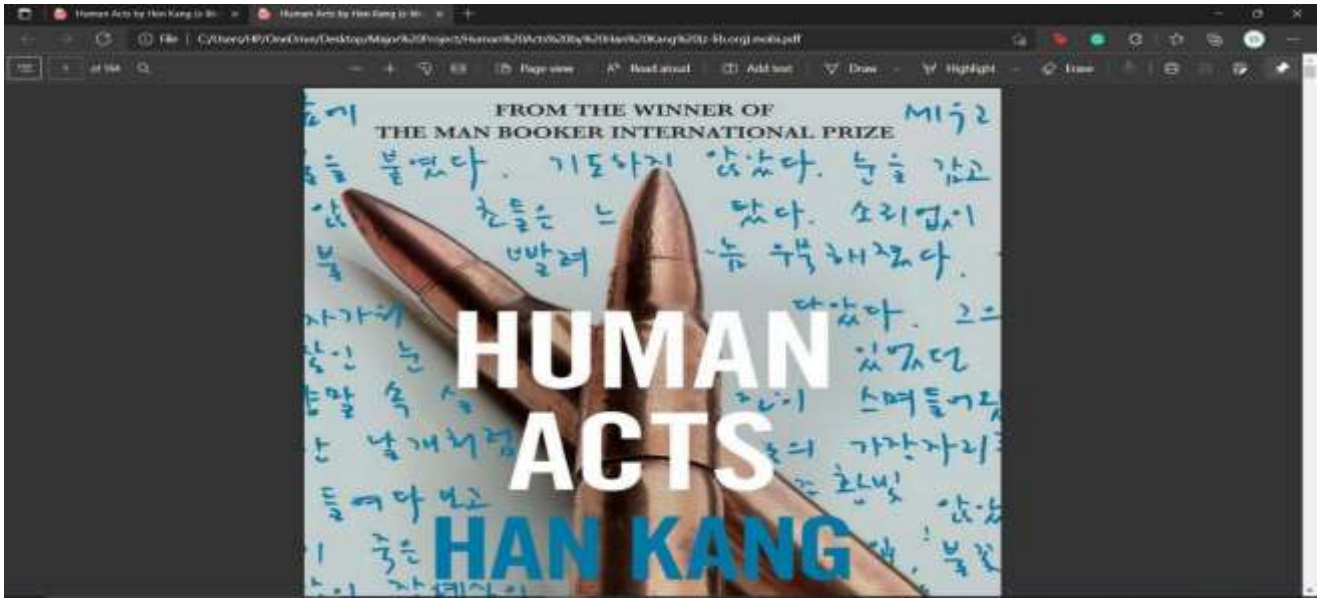

Fig 7: Results Page

5.CONCLUSION

The suggestion in this study is to ensure the confidentiality of cloud-stored data by integrating digital signatures and Diffie Hellman key exchange with the (AES) Advanced Encryption Standard encryption technology. Even if the key in transit is compromised, the Diffie Hellman key exchange facility renders it ineffective because the key in transit is useless without the user's private key, which is only accessible to the legitimate user. This proposed three-way strategy makes it impossible for hackers to breach the security system, hence safeguarding cloud data.

REFERENCES

[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.

[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 medicineand education.

[5] Farhan Bashir Shaikh and Sajjad Haider "Security Threats in Cloud Computing" 2011 IEEE 6th international conference on Internet Technology and secured transactions, 11-14 December 2011, Abu Dhabi United States of Arab Emirates.

[6] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, "Cloud Security Issues" 2009 IEEE International Conference on Services omputing.