TITLE**: Use of Digital Signature with DiffieHellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing**

**AUTHOR**: PrashantRewagad, YogitaPawar.

Cloud computing is the apt technology for the

decade. It allows user to store large amount of data in cloud

storage and use as and when required, from any part of the

world, via any terminal equipment. Since cloud computing is

rest on internet, security issues like privacy, data security,

confidentiality, and authentication is encountered. In order to

get rid of the same, a variety of encryption algorithms and

mechanisms are used. Many researchers choose the best they

found and use it in different combination to provide security to

the data in cloud. On the similar terms, we have chosen to

make use of a combination of authentication technique and key

exchange algorithm blended with an encryption algorithm.

This combination is referred to as “Three way mechanism”

because it ensures all the three protection scheme of

authentication, data security and verification, at the same time.

In this paper, we have proposed to make use of digital

signature and Diffie Hellman key exchange blended with

(AES) Advanced Encryption Standard encryption algorithm to

protect confidentiality of data stored in cloud. Even if the key

in transmission is hacked, the facility of Diffie Hellman key

exchange render it useless, since key in transit is of no use

without user’s private key, which is confined only to the

legitimate user. This proposed architecture of three way

mechanism makes it tough for hackers to crack the security

system, thereby protecting data stored in cloud.

Cloud computing is the apt technology for the

decade. It allows user to store large amount of data in cloud

storage and use as and when required, from any part of the

world, via any terminal equipment. Since cloud computing is

rest on internet, security issues like privacy, data security,

confidentiality, and authentication is encountered. In order to

get rid of the same, a variety of encryption algorithms and

mechanisms are used. Many researchers choose the best they

found and use it in different combination to provide security to

the data in cloud. On the similar terms, we have chosen to

make use of a combination of authentication technique and key

exchange algorithm blended with an encryption algorithm.

This combination is referred to as “Three way mechanism”

because it ensures all the three protection scheme of

authentication, data security and verification, at the same time.

In this paper, we have proposed to make use of digital

signature and Diffie Hellman key exchange blended with

(AES) Advanced Encryption Standard encryption algorithm to

protect confidentiality of data stored in cloud. Even if the key

in transmission is hacked, the facility of Diffie Hellman key

exchange render it useless, since key in transit is of no use

without user’s private key, which is confined only to the

legitimate user. This proposed architecture of three way

mechanism makes it tough for hackers to crack the security

system, thereby protecting data stored in cloud.

Cloud computing is the relevant technology for this decade. It allows users to store huge amount of data in cloud storage and use as and when required, from anywhere in the world, through any kind of terminal equipment. Since cloud computing relies on internet, cloud data will be forced to contend with security issues like privacy, data security, confidentiality, and authentication. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. This paper, introduces use of hybrid cryptographic algorithm blended with digital signature and Diffie Hellman key exchange.. The hybrid algorithm is designed using the combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user’s private key, which is confined only to the legitimate user. This proposed architecture of hybrid algorithm makes it tough for hackers to crack the security and integrity of the system, thereby protecting data stored in cloud.

**TITLE**: **Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing**.

**AUTHOR**: Uma Somani, Kanika Lakhani, ManishaMundra

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 computing is 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.

**TITLE**: **Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing**.

**AUTHOR**: Mehdi Hojabri& Mona Heidari

The Cloud Computing is the next generation platform that provides dynamic resources pools, virtualization, and high availableness. Today, with the assistance of those computing, we are able to utilize ascendable, distributed computing environments among the boundary of the web, It provides several edges in terms of low value and accessibility of information, conjointly offers associate degree innovative business model for organizations to adopt It’s services while not forthright investment. Except for these potential gains achieved from the cloud computing, there are plenty of security problems and challenges related to it and conjointly knowledge privacy protection and knowledge retrieval management is one in all the foremost difficult analysis add cloud computing. To supply security a range of cryptography algorithms and mechanisms are used. Several researchers opt for the simplest they found and use it numerous combinations to supply security to the information in cloud. In this paper, we’ve got planned to form use of Digital signature and Kerberos with Advanced Encryption Standard cryptography (AES) algorithm program to guard Authentication, Confidentiality, and Integrity of information hold on in cloud.

**TITLE**: **Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm.**

**AUTHOR**: Ashish Prajapati, Amit Rathod.

Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services, etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services providers’ servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters.