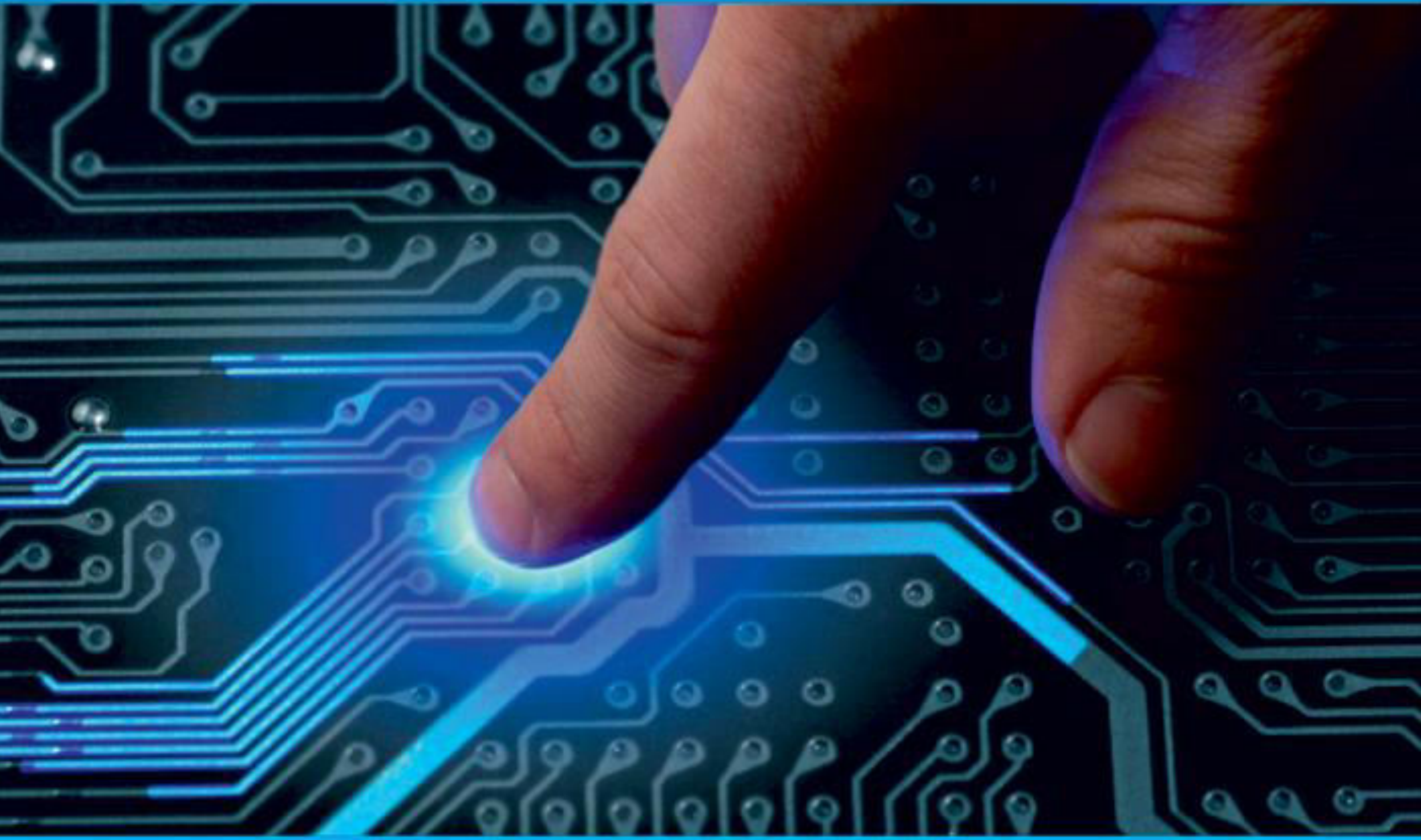
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 10, October 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 10, October 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1110038 |

# Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing

**Samvedhya Bendapudi**

Student, Department of Computer Science and Engineering, GITAM University Vishakapatnam, India

**ABSTRACT:** The cloud is the perfect technology for the coming decade. It lets the user to store a significant amount of data in the cloud and access it from any location, using any type of terminal equipment, whenever necessary. Privacy, data protection and secrecy, as well as authentication and access control are difficulties that cloud computing presents. Various encryption techniques and mechanisms are employed in order to get rid of the troublesome issue. Many researchers pick the best of what they've uncovered and use it in various ways to secure cloud data. An encryption algorithm and an authentication technique are used together in the same way that we use a key exchange algorithm and an encryption algorithm. Three-way mechanism" refers to the fact that authentication, data security, and verification are all protected simultaneously. In this research, we suggest using the Advanced Encryption Standard (AES) encryption method in conjunction with digital signatures and Diffie Hellman key exchange to ensure the secrecy of data stored in the cloud. If the key in transit is compromised, Diffie Hellman key exchange renders it ineffective because the key in transit is meaningless without the user's private key, which can only be accessed by authorised users. In order to protect cloud-based data, a three-way technique has been devised that is difficult for hackers to break.
Cloud Computing, AES Algorithm, and Data Confidentiality are all used in this report.

## I. INTRODUCTION

Internet computing is the simplest definition of cloud computing. People and companies can think of cloud computing as using the internet to deliver technology-enabled services to individuals and businesses.[5] For many businesses, cloud computing is a new resource that may help them function more efficiently. Shared computer resources are implied in order to manage software. When it comes to delivering services at different abstraction levels, such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service), cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability[6]. A wide range of applications, including financial portfolios that provide tailored information, and computer games that immerse players, are powered by this technology. It's a pay-as-you-go service, therefore it's quickly gaining traction. User privacy, data theft and leakage, eavesdropping, unauthenticated access, and numerous hacker assaults have been raised because cloud computing is a service that can be accessed through the Internet. Cloud computing adoption has been stymied by security concerns related to identification, privacy, data protection, and data verification. Thus, we have presented a secure cloud computing architecture in order to get widespread support in the financial, market, and industry sectors.

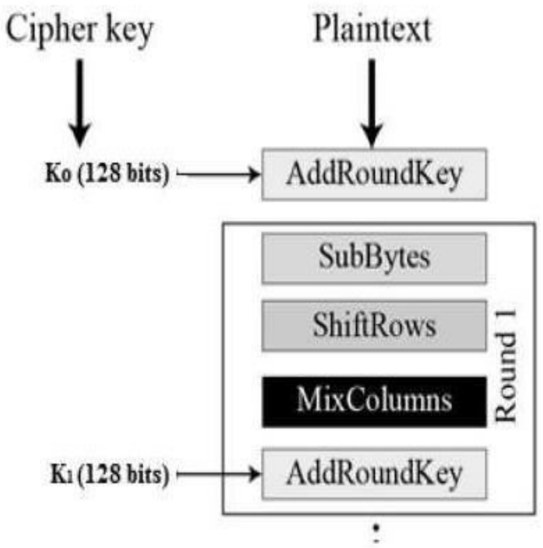


Fig.1: Encryption process

The three most often used cloud computing service models are outlined here.
ASP (Application Service Provider) is another name for the SaaS paradigm. It is a service that enables customers to use simple software, such as a browser, to access cloud-based services. Gmail and Google Groups are two examples.
2. Platform as a Service (PaaS): This service enables customers to design and deploy applications. Google App Engine, for example, enables developers to build their own bespoke apps.
User access to servers' computational and storage infrastructure is made possible through Infrastructure as a Service, or IAAS. [2] Three and six are both correct. Let's use Amazon Web Services as an illustration. Amazon.com's computing services can be accessed from a distance with this tool.
Security, privacy, liability, and dependability are just a few of the major policies that govern the cloud computing industry [2]. Data security and how cloud service providers ensure it is the most critical of these challenges [2]. Encryption is the best way to keep our data safe. For many years, several encryption systems have been used to protect data. The process of encrypting data is accomplished by transforming plaintext into ciphertext. As the conversion process necessitates large and sophisticated mathematical calculations, this strategy isn't very effective when used with cloud computing systems.

## II. LITERATURE REVIEW

### *2.1 Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing [1] :*

Dynamic resource pools, virtualization and high availability are only some of the benefits of cloud computing. As a result of the advent of cloud computing, it is now possible to use scalable, distributed computing systems over the Internet. In order to alleviate common computer issues such as hardware, software, and resource availability for on-demand use, the cloud computing concept was developed. When it comes to everyday computing, the cloud offers a convenient and cost-effective alternative. Security and the proper implementation of Cloud Computing across the network are the most common Cloud Computing issues. A digital signature with the RSA technique was used in this research paper to evaluate cloud storage methods and data security in the cloud.
This section focuses on cloud networking's security architecture.
There are numerous advantages to using the cloud, such as reduced capital expenditures, operational hazards and complexity, and enhanced scalability while providing services at different abstraction levels — specifically SaaS, PaaS and IaaS. (IaaS). Introducing cloud networking, a novel method to cloud computing that adds networking features to cloud computing, allows for dynamic and flexible placement of virtual resources across provider borders. Such optimizations include lowering latency or network burden, for example. In addition, this technique raises significant security concerns. Cloud networking users will be able to specify and enforce security requirements in the infrastructure by using the security architecture described in this paper.

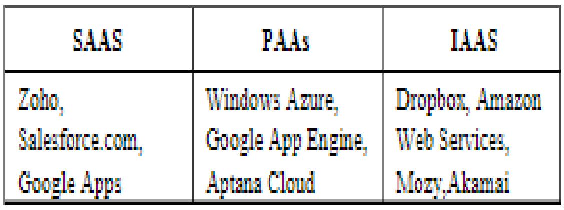
In the cloud, there are a number of security and privacy concerns.

Many businesses are moving their applications and data to the public or hybrid cloud because of the many benefits that cloud computing can provide. Although some vital business applications, such as those used by large corporations, would not be moved to the cloud, firms still choose to keep them on-premises. In comparison to expectations, cloud computing's proportion of the industry is still a long way off. Data security and privacy protection concerns remain the key barrier to cloud computing adoption from the standpoint of customers. This paper provides a succinct but comprehensive study of cloud computing-related data security and privacy protection challenges at all phases of the data life cycle. Afterwards, this paper explores a few of the most recent options. Last but not least, this paper describes upcoming research on cloud-based data security and privacy challenges.

4. Research on a Multidimensional Cloud Computing Data Security Model:

It is generally agreed that cloud computing represents the next step in the evolution of the information technology frameworks. Dynamic resource pools, virtualization, and high availability can all be provided by the next generation of computing platforms. In the present cloud computing system, there are a number of new security issues that haven't been taken into account. Because of this, the foundation for building a cloud computing security system is a cloud computing data security system. Consequently The cloud computing technological architecture and cloud computing data security aspects are first examined and discussed in this article, before the cloud computing data security model is raised. Finally, there has been investigation into the implementation of a data security paradigm. The model has a three-layered protection system. To begin, user authentication is necessary in order to prevent unauthorised access to personal information. Data addition, modification, and deletion are all possible for users who successfully complete the authentication process. Unauthorized users who take advantage of the authentication system's flaws may gain access to sensitive data. This layer encrypts the user's data. If the intruder has obtained the key, there is cause for concern. Even if the user data is received via a privacy protection function, no useful information may be gleaned from it. For commercial cloud computing users, protecting their corporate secrets is critical. Last but not least, there is the file quick regeneration layer, which ensures that even if a user's data is corrupted, it will be restored as quickly as possible thanks to this layer's rapid regeneration method. Each layer serves a specific purpose and works together to ensure cloud computing data security.

Cloud Computing Randomness and Performance Testing 2.5 Modern Encryption Techniques:
Cloud computing must be the IT Enterprise's next-generation infrastructure. Clouds are enormously complicated systems. Primitive elements, which are repeated hundreds of times, can be reduced to common functional units. There are a lot of concerns with cloud computing because of how complicated it is, including a lot of security issues. Data security is one of the most critical topics. When a cloud service has a single security design, but has a large number of customers with varying needs, it can be difficult to protect. Data storage security is the primary focus of the suggested research. For both cloud computing and traditional desktop applications, data security is a major consideration. This is to ensure the best level of privacy possible. Cloud computing's data security relies heavily on modern encryption methods. RC4, RC6, MARS, AES, DSS, 3DES, and Two-Fish and Blow-Fish are all evaluated on two separate platforms, a desktop computer and an Amazon EC2 Micro Instance cloud computing environment, respectively. NIST statistical testing has been used to evaluate the randomness of these encryption methods in a cloud computing context. In order to establish the best appropriate technique and analyse the performance of several modern encryption algorithms, this study makes use of a pseudo-random number generator (PRNG). It is possible to implement cryptographic algorithms using the Java Cryptography Extensions framework (JCE). The efficiency of each algorithm is demonstrated by simulation results.



| SAAS | PAAs | IAAS |
|---|---|---|
| Zoho,<br>Salesforce.com,<br>Google Apps | Windows Azure,<br>Google App Engine,<br>Aptana Cloud | Dropbox, Amazon<br>Web Services,<br>Mozy,Akamai |

Fig.2: Example of cloud providers with service

***2.6 An Analysis of The Cloud Computing Security Problem [10]:***

New paradigm of computation, called "the cloud," allows enterprises to use IT without making large upfront investments. Despite the potential benefits of cloud computing, the security of the model remains uncertain, which has an impact on the adoption of the cloud model. The cloud model introduces new aspects to the security problem, such as multi-tenancy, elasticity, and layered dependency stack, into the problem area. In this paper, we provide a comprehensive examination of the issue of cloud security. We looked at the issue from a variety of angles, including the cloud architecture, the cloud features, the cloud stakeholders, and the cloud service delivery methods. We can then use this information to develop a comprehensive description of the cloud security issue and a list of essential characteristics that should be included in any security solution we develop.

## III. IMPLEMENTATION

Data and services can be used and stored in any location outside of an organization's direct jurisdiction using cloud computing. Privacy, confidentiality, integrity, and other security concerns arose as a result of this facility, which necessitated a secure computer environment. A system that authenticates, verifies, and encrypts data is needed to engender trust in computing, thus ensuring data secrecy.
Protective measures are employed in three different ways in our proposed design. First, keys for the exchange stage are generated using the Diffie Hellman method. Digital signature is used to authenticate users, and subsequently AES encryption is utilised to encrypt or unlock user data files. All of this is done to ensure a secure computing environment so that data cannot be tampered with at the server end. Additionally, a (trusted) computing platform is used to encrypt user data files and a storage server is used to store user data files. In order to upload a file to the cloud server, a user must first log in and exchange keys using Diffie Hellman key exchange before their digital signature can be verified. Once AES has been used to encrypt the user's data file, the file is then uploaded to another (cloud) Storage server. When a client needs the same file again, the cloud server is where it will be downloaded from. In order to accomplish this, when a user logs in, he or she first exchanges encryption keys, selects a file to download, authenticates using a digital signature, and finally uses AES to decrypt the saved file.

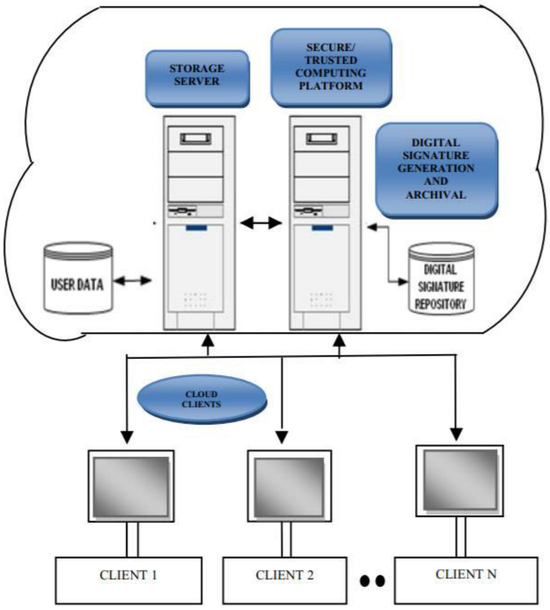

STORAGE SERVER
SECURE/ TRUSTED COMPUTING PLATFORM
DIGITAL SIGNATURE GENERATION AND ARCHIVAL
USER DATA
DIGITAL SIGNATURE REPOSITORY
CLOUD CLIENTS
CLIENT 1
CLIENT 2
CLIENT N

Fig.3: System architecture

1. Exchange Keys • Authenticate Signatures • Client Authentication
In order to upload data, you must first create an account
• Data Download
• Logout
Server for Cloud-based Storage
The third option is to use a cloud server.
First, keys for the exchange stage are generated using the Diffie Hellman method. Digital signature is used to authenticate users, and subsequently AES encryption is utilised to encrypt or unlock user data files. All of this is done in order to deliver a dependable service. First, keys for the exchange stage are generated using the Diffie Hellman method. Digital signature is used to authenticate users, and subsequently AES encryption is utilised to encrypt or unlock user data files. All of this is done in order to provide a solid foundation of confidence for users.

## IV. ALGORITHMS

### DIFFIE-HELLMAN ALGORITHM:

Using the elliptic curve to generate points and the parameters to obtain the secret key, the Diffie-Hellman algorithm is being used to build a shared secret for secret conversations across a public network. There are four variables in the algorithm: a prime (P), a primitive root (G), and two private values (A and B). In both cases, the numbers P and G are publicly accessible Each user chooses two private values (let's say Alice and Bob), then generates their own unique key and shares it with the other user(s). The other person obtains the key, and that generates a secret key, after which they have the same secret key to encrypt with.

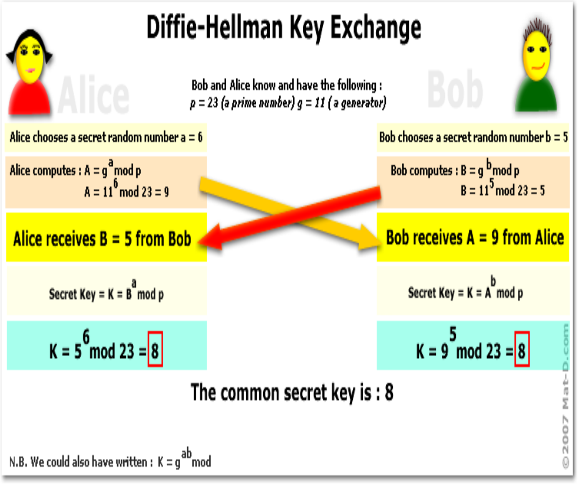

Diffie-Hellman Key Exchange
Alice
Bob
Bob and Alice know and have the following :
p = 23 (a prime number) g = 11 ( a generator)
Alice chooses a secret random number a = 6
Bob chooses a secret random number b = 5
Alice computes : A = g^a mod p
A = 11^6 mod 23 = 9
Bob computes : B = g^b mod p
B = 11^5 mod 23 = 5
Alice receives B = 5 from Bob
Bob receives A = 9 from Alice
Secret Key = K = B^a mod p
Secret Key = K = A^b mod p
K = 5^6 mod 23 = 8
K = 9^5 mod 23 = 8
The common secret key is : 8
N.B. We could also have written : K = g^ab mod
©2007 Mat-D.com

Fig.4: Diffie hellman key exchange

### DIGITAL SIGNATURE SHA-1:

As a message digest, SHA-1 generates a 160-bit (20-byte) hash value from an input using a cryptographically broken but still frequently used hash algorithm. This hash value is typically represented by an octal number with 40 decimal places. As an official U.S. Federal Information Processing Standard, it has been established and implemented by the National Security Agency. Because of its vulnerability to well-funded adversaries since 2005, various groups have advocated that SHA-1 be replaced. It was publicly deprecated by NIST in 2011 and digital signatures were banned from using SHA-1 in 2013. It is possible to conduct chosen-prefix attacks on SHA-1 by the year 2020. As a result, SHA-1 should be replaced with SHA-2 or SHA-3 as soon as practicable. When it comes to digital signatures, SHA-1 needs to be replaced immediately. SHA-1 SSL certificates were no longer accepted by popular web browsers in 2017. SHA-1 was the target of a collision attack by CWI Amsterdam and Google in February 2017. They published two distinct PDF files that produced the identical SHA-1 hash. It's still safe to use SHA-1 for HMAC.

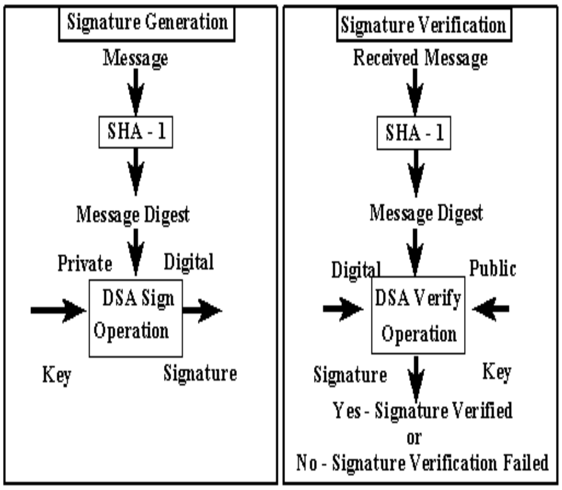


Fig.5: SHA-1 figure

**ADVANCED ENCRYPTION STANDARD (AES):**

Today, the most common and extensively used symmetric encryption technique is Advanced Encryption Standard (AES) (AES). At least six times faster than triple DES, it is discovered. The key size of DES has to be increased since it was becoming insecure. It was thought to be vulnerable to an exhaustive key search attack because of the rise in computing power. In order to get around this problem, the Triple DES algorithm was created.

AES has the following features:

∟Symmetric block cypher with a symmetric key

Keys with 128/192/256-bit lengths

More secure and faster than Triple-DES encryption.

Specification and design information should be provided in full.

Software that can be written in both C and Java.

An iterative rather than a Feistel cypher, AES is used in place of AES. Based on the "substitution–permutation network," it can be applied to many problems. There are several linked processes that do replacements and shuffle bits around, some of which replace inputs with specific outputs (substitutions) (permutations). Bytes rather than bits are used in AES's computations. As a result, AES considers a plaintext block of 128 bits as 16 bytes. Four columns and four rows of 16 bytes are arranged in a matrix for easy processing. AES has a configurable number of rounds based on the length of the key, unlike DES. For 128-bit keys, AES utilises 10 rounds; for 192-bit keys, it uses 12 rounds; and for 256-bit keys, it uses 14 rounds. The original AES key is used to generate a new 128-bit round key for each subsequent round.

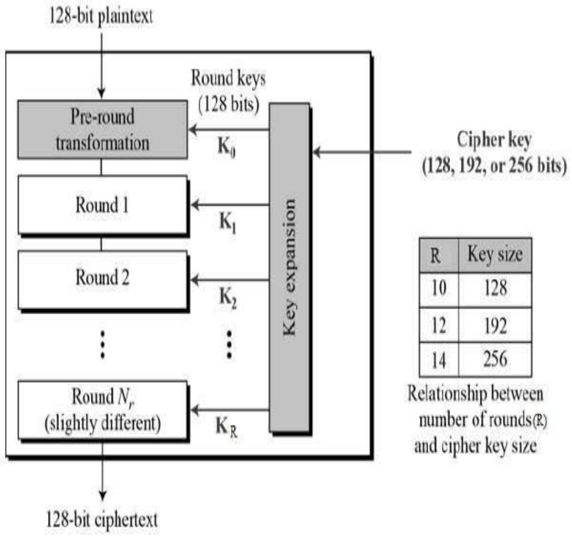


Fig.6: AES structure

AES is widely used and supported in both hardware and software in modern encryption. Until now, no realistic cryptanalytic attacks have been uncovered against the AES algorithm. To counteract improvements in the ability to execute exhaustive key searches in the future, AES features a built-in ability to adjust the length of its keys. In the same way that excellent key management is essential for DES, good implementation is critical for AES security.

## V. EXPERIMENTAL RESULTS

As the original method of exchanging public keys, the Diffie-Hellman key exchange protocol has a lot of historical significance. [8] In 1976, Witfield Diffie and Martin Hellman put out the idea. It has two private and one secret key. Encryption is done with a private key and the sender's public key if the recipient wishes to communicate. On the receiving end, the recipient uses his private key and the sender's public key to decode the message. [8] The difficulty of calculating logarithmic functions for prime exponents is the basis for this strategy. As the name suggests, this is called the Discrete Logarithm Problem (DLP) [11].

Key generation is an integral aspect of the process. Both the public and the private key should be generated using an algorithm. The sender will use the recipient's public key to encrypt the message contents, and the recipient will use its own private key to decrypt it.

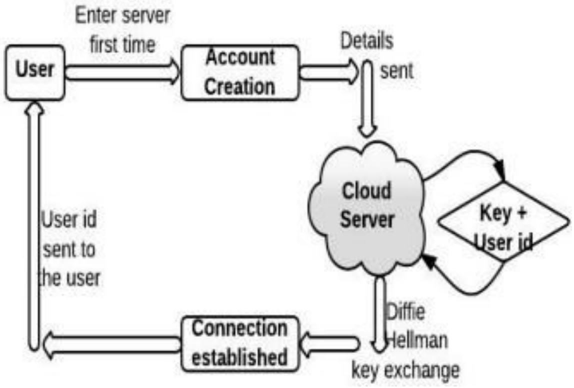


Fig.7: Account creation process

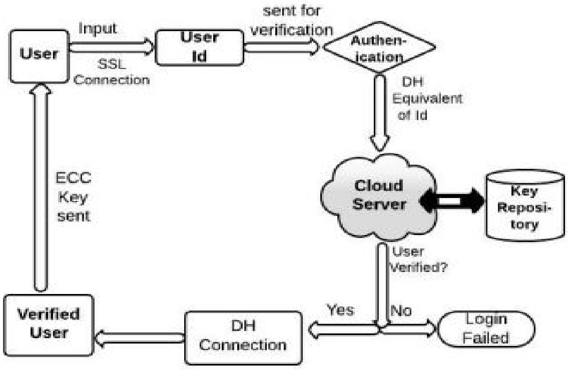


Fig.8: Authentication of user

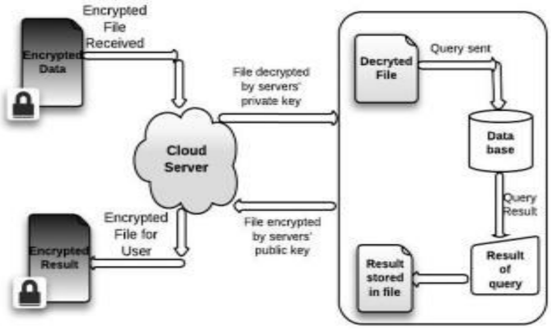


Fig.9: Data Processing view of Server

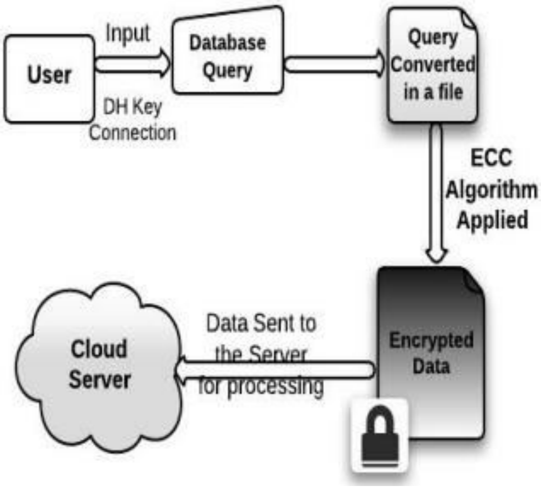


Fig.10: Data Processing view of Client

## VI. CONCLUSION

In this research, we suggest using the Advanced Encryption Standard (AES) encryption method in conjunction with digital signatures and Diffie Hellman key exchange to ensure the secrecy of data stored in the cloud. No matter how well-known the Diffie Hellman exchange facility is, it will be worthless even if a key in transit is compromised, as the private key of a genuine user is required to decipher it. In order to protect cloud-based data, a three-way technique has been devised that is difficult for hackers to break.

## VII. FUTURE SCOPE

To demonstrate the effectiveness of our proposed design in the future, we will focus on implementing it and conducting various comparisons.

## 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 medicine and 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 Computing.

[7] Ayesha Malik and Muhammad Mohsin Nazir ”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 , Eman m.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.

[11] Aqeel Khalique Kuldip Singh Sandeep Sood. Implementation of Elliptic Curve Digital Signature Algorithm. International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[12] Alfred Menezes, Minghua Qu, Doug Stinson, Yongge Wang. Evaluation of Security Level of Cryptography: ECDSA Signature Scheme. Certicom Research. January 15, 2001.

[13] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[14] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.

[15] Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85.

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING