IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 3, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

# Attribute Data Encryption and Decryption Technique for Cyber Security in Cloud Environment

[1]Muttappa Mantur, [2]Dr. Amit Jain

[1]Research Scholar, Department of Computer Science and Engineering, SunRise University, Alwar, Rajasthan, India

[2]Research Supervisor, Department of Computer Science and Engineering, SunRise University, Alwar, Rajasthan, India

**ABSTRACT:** Cloud computing is one of the most important advances in information technology, but data storage security issues are a major concern in cloud environments. Data protection includes data integrity, data reliability, data confidentiality, etc. Despite the various measures taken to protect data, such as encryption and decryption, the data is exposed to potential security risks. Encryption is the art and science of encrypting messages to render them unintelligible and ensure privacy. Cloud data comes from various sources. How secure is my data? Data security issues are rapidly increasing as data flows over the Internet. To protect sensitive information, there are many encryption techniques to hide data from unauthorized users. Encryption and decryption methods are used to protect data and only authorized users can access it. However, in some cases, brute force methods can reveal hidden data. To improve data confidentiality and authentication issues, attribute data encryption and decryption techniques for cybersecurity in cloud environments are introduced. Attribute-based encryption is a promising technology that enables flexible and fine-grained data access control over encrypted data, and is well suited for secure data exchange environments such as cloud computing, which is currently prevalent. . Attribute-based security schemes help provide significantly faster response times and higher throughput authentication.

**KEYWORDS:** Cloud Computing, Data Security, Cryptography, Encryption and Decryption.

## I. INTRODUCTION

Cloud computing is a utility for data storage. Data storage security has become a primary challenge. The users can access, share & transacts the data as the cloud offers services based on the user demand [2].

With the fast advancement in cloud computing, progressively more users store their applications and data on the cloud. Cloud computing has lots of features, e.g. virtualization, multi-user, efficiency, cost savings, and most importantly security [3]. Cloud computing is used as data storage so data security and privacy issues such as confidentiality, availability and integrity are important factor associated with it. Cloud storage provides user to access remotely store their data so it becomes necessary to protect data from unauthorized access, hackers or any type of modification and malicious behavior. Security is an important concern. The meaning of data storage security is to secure data on storage media. Cloud storage does not require any hardware and software management as it provide high quality applications [4].

Security being the most important factor in cloud computing has to be dealt with great precautions. A high requirement arises for security and protection of data from any unauthorized user as leakage of confidential information may result in serious impairment to user. This increases the security requirement of confidential data before actually migrating it over online internet access. A sound, safe and secure framework is need to be developed to protect the confidential data from any such malicious attack. There is a need to convert confidential data into some another form, which becomes inexplicable for any attacker and only authorized users are able to understand that exactly what data is communicated. One of the major techniques to achieve this requirement is cryptography, also known as "code making" or "code generation". It allows us to translate a message into unreadable form for malicious attacker [7].

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

Cryptographic mechanism is considered a proper solution and a basic tool to guarantee data security (i.e., confidentiality, integrity, and authentication). It concerns about using symmetrical numbers with private key and asymmetrical numbers with public key. There are some Cryptography algorithms have been existed such as block ciphers (e.g., AES, DES, 3DES, and Blowfish algorithms), and stream ciphers (e.g. Rivest Cipher 4 (RC4), Rivest Cipher 5 (RC5), Rivest Cipher 6 (RC6) and One Time Pad (OTP) algorithms [10].

Cloud computing is a growing technology that provides an opportunity for customers, who does not need to waste money in purchasing the hardware resources. Nowadays, privacy and security are the most important issues for setting up a cloud. If a cloud service provider ensures reliable and secure services, customers can easily access cloud services. In order to provide data security, all data must be encrypted before being stored on a cloud server [8].

In order to improve the security of data transmission, encryption is essential Encryption resolves this problem to a great extent by ensuring that the data is not decipherable during transfer. Encryption converts data into another form, which can only be deciphered by users with the respective keys or other access mechanisms. Encrypted data is commonly called ciphertext, while decrypted data is plain text. Encryption can be broadly classified into symmetric encryption, public-key encryption, and asymmetric encryption, also known as private-key encryption. When encryption and decryption are performed using the same key for both functions, it is called symmetric key encryption, whereas, for asymmetric encryption, a public-private key pair is generated where public key encrypts and private key decrypts the data.

The cryptogram scheme and encryption algorithm cannot be kept absolutely secret nowadays, once the keys are obtained by the opposite side or go wrong, the whole security system will be cracked down catastrophically. Therefore, the saying that all secrets are implied in the keys has become a basic principle for modern cryptography. To a great extent, the security of the modern security system depends on the key and key management.

To generate keys is the first part of three important factors in the key management system, and it is the beginning of the keys management. The quality of the keys directly plays a very important role in the security of the key management. Besides, it produces a great impact on the security performance of the whole security system. Therefore, to generate high performance keys is crucial to the system security. The high-quality keys can't be generated repeatedly, and there is high demand for the randomness and unprediction. Many encryption techniques have been presented to cope with data security issues. However still there is a gap which needs to improved with advanced encryption and key generation techniques [1].

Millions of users can access data on a cloud. At the same time, it is essential to secure their data by producing same number of cryptographic keys. In this context, key generation and management is crucial to the protection of cloud data [9]. To maintain sensitive information and confidentiality in cloud computing is of great importance which means the need for more robust ways to keep it from the attackers. In this work, Attribute Data Encryption and Decryption Technique for Cyber Security in Cloud Environment is presented.

The rest of the work is organized as follows: The section II describes the literature survey. The section III presents Attribute Data Encryption and Decryption Technique for Cyber Security in Cloud Environment. The section IV presents the result analysis of presented approach. Eventually the work is concluded in section V.

## II. LITERATURE SURVEY

Zhenyong Zhang, Peng Cheng, Junfeng Wu, Jiming Chen et. al., [11] describes Secure State Estimation Using Hybrid Homomorphic Encryption Scheme. Armed with encryption, ESE (Encryption Based Estimation) is able to conceal comprehensive information (i.e., model parameters, measurements, and estimates) aggregated at the estimator while retaining the correctness of the normal state estimation. Therefore, even if an attacker has gained unauthorized access to the estimator and associated communication channels, he/she will not be able to obtain sufficient knowledge of the system state to guide the attack. Furthermore, due to the encryption-induced quantization error, we give a sufficient stability condition for ESE. Finally, we implement ESE with real world hardware to illustrate its effectiveness and efficiency.

Shweta Kaushik, Ashish Patel et. al., [14] describes Secure Cloud Data Using Hybrid Cryptographic Scheme. They present a hybrid symmetric encryption approach to provide more security for owner's data other than any single

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

symmetric encryption algorithm. This use of hybrid approach makes data more secure and protect it from any malicious activity attended by intruder. Brute force attack also becomes impossible after using this proposed approach. Use of symmetric encryption also increases the processing ability as it has fast processing speed and efficient than asymmetric approach.

Nadia Mohammed; Najla Ibrahim, et. al., [16] presents implementation of New Secure Encryption Technique for Cloud Computing. In this work, several levels of multi-coding levels were developed using more than one method to obtain more confidentiality through DNA (Deoxyribonucleic Acid) encryption and adding a higher level of confidentiality by adding Advanced Encryption Standard (AES) and then loading it into the cloud storage. A Matlab program (R2014a) has been used for implementing proposed scheme with several analyses. The analyses show that proposed scheme has a convincing level of security, efficiency, complexity and speed.

Siddharth Singh, Varun Kumar, UtkarshVerma, Azhagiri M et. al., [17] describes Data Security in Cloud Computing Using Cryptographic Algorithms. This paper deals with the use of AES algorithm in PaaS cloud computing service. By using AES calculation has a high security level since the bits utilized are the 128, 192 or 256-piece key. It indicates obstruction against a large group of assortment of assaults to be specific square assault, key assault, key recuperation assault and differential assault. In this manner, AES calculation is a profoundly secure encryption technique existing in the encryption showcase. When the information is encoded with AES, it can likewise ensure against future assaults, for example, crush assaults. AES encryption calculation utilizes insignificant extra room and yields superior exhibitions with no shortcomings.

Kavita Saini, Vaibhav Agarwal, Arjun Varshney, Anushka Gupta et. al., [18] describes E2EE for Data Security For Hybrid Cloud Services: A Novel Approach. The paper also explores the functionality and drawback of AES Algorithm and MD5 (message Digest-5) approaches. This approach discusses the novel approach of End to end encryption for data security for hybrid cloud services and also discuss the functionality and shortcomings of this technology. It is used to send the data without reading the original data, but encryption of the data is followed by the Public key & on the other hand, Decryption is followed by the Private Key. By doing this the server never sees the plaintext message and steal the data. The paper concluded that E2EE (End to End Encryption) is one of the good approaches for hybrid security.

Vishwanath S Mahalle; Aniket K Shahade et. al., [19] describes Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. This paper presents Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. This paper mainly focuses on the following key tasks: 1. Secure Upload of data on cloud such that even the administrator is unaware of the contents. 2. Secure Download of data in such a way that the integrity of data is maintained. 3. Proper usage and sharing of the public, private and secret keys involved for encryption and decryption. The use of a single key for both encryption and decryption is very prone to malicious attacks. Out of the three keys one is the public key, which is made available to all, the second one is the private key which lies only with the user. In this way, both the secure upload as well as secure download of the data is facilitated using the two respective keys. This has helped in avoiding any chances of repeated or redundant key.

## III. ATTRIBUTE DATA ENCRYPTION AND DECRYPTION TECHNIQUE

In this section, Attribute Data Encryption and Decryption Technique For Cyber Security in Cloud Environment is presented. The workflow of presented approach is shown in Fig. 1. Industrial environments involve too many components to collect and store data in a cloud-computing model, e.g., sensors, smart phones, signage, servers, control servers, databases, etc. Once the data has been collected with the support of internet connection, the information is held in the cloud-computing environment. Furthermore, a cloud has layered architecture. This approach works on the service layer of a cloud-computing environment as it manages databases, servers, message queues, etc. The cloud includes decision makers, implementers, maintainers and users.

Gartner for Technical Professionals clients that enable IT practitioners and technical teams to make smarter and faster cloud vendor decisions. The Cloud Computing for Decision-makers and Leaders journey is targeted at decision-makers and leaders, empowering participants to advance their enterprises' cloud initiatives. Learners will be able to define and describe the history of information technology leadership in the context of cloud computing. What's critical here is that the learner knows how to compare and contrast the older traditional ways of decision-making in preparation for their new cloud computing leadership role.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

The cloud has various deployment and service models that can help an organization design their very own cloud strategy based on their needs. The decision makers will know about components of cloud computing including storage, compute, data management, monitoring, code management, and process and deployment management. Decision making is a dynamic process that helps in aggregating significant algorithms and most secure algorithms. Cloud implementation service is the wholesome activity involved in integrating your business operations with cloud computing services. It goes beyond moving data and applications into the management and customizations to meet your business goals.

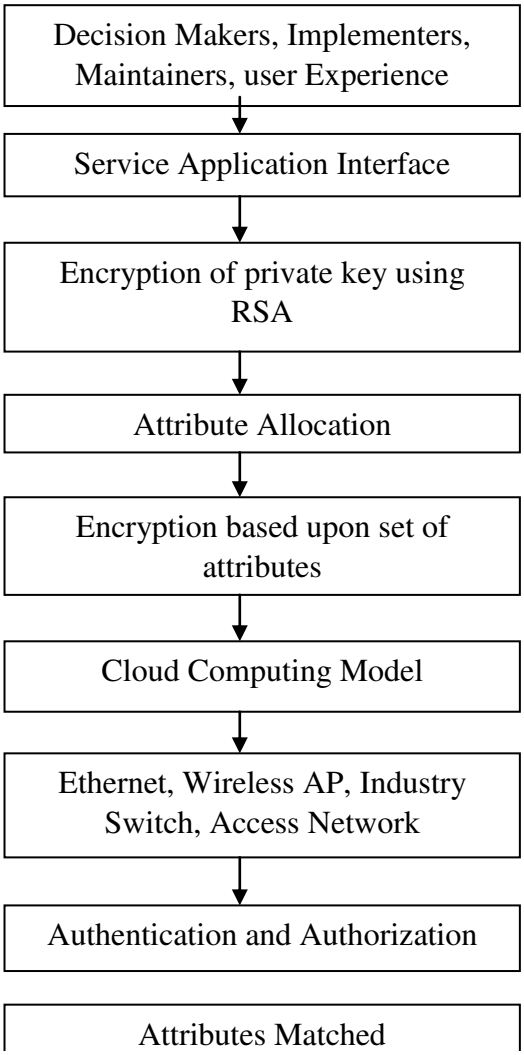


**FIG. 1: BLOCK DIAGRAM OFATTRIBUTE DATA ENCRYPTION AND DECRYPTION TECHNIQUE**

Cloud computing operation and maintenance is the process of managing the cloud infrastructure, applications, and data. It involves the monitoring of the system performance, the security of the system, and the maintenance of the system. User experience (UX) focuses on having a deep understanding of users, what they need, what they value, their abilities, and also their limitations. User experience (UX) is a concept in computing system and application design that studies

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

and evaluates human feelings and expressions when using such systems. UX facilitates and enables the development of computing systems that are centered on ease of use and accessibility for a human user.

A Cloud service API is a software interface that allows developers to link cloud computing services together. Application programming interfaces (APIs) allow one computer program to make its data and functionality available for other programs to use. Developers use APIs to connect software components across a network. It enables applications to communicate and transfer information to one another in the cloud. It is a software program where cloud-based and local components work together. This model relies on remote servers for processing logic that is accessed through a web browser with a continual internet connection.

Encryption: The secret data upload to the cloud will be encrypted using ABE. RSA is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm. RSA is a type of asymmetric encryption, which uses two different but linked keys. In RSA cryptography, both the public and the private keys can encrypt a message. The opposite key from the one used to encrypt a message is used to decrypt it. The main advantage of RSA is if the attacker decrypts the data of RSA cipher then it will give the results but that results will be different from the original data.

Private key K is generated using RSA. In this step the private key encryption will be done to make the decoding of data more difficult. RSA technique will be used to encrypt the private key. Here are the following steps: K representing the key as integer K $\epsilon${0....n-1}.Compute

$$C = K^e mod n \quad (1)$$

Before decrypting the encrypted data, the authenticated user at receiver end should have to decrypt the private key to obtain the original data. Here the following steps are:-

$$K = C^d mod n \ (2)$$

Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. Attribute-based encryption is a generalisation of public-key encryption which enables fine grained access control of encrypted data using authorisation policies. The secret key of a user and the ciphertext are dependent upon attributes.

The attributes includes identity, authentication, authorization, integrity, confidentiality, non-repudiation, and basic message exchange. Attribute-based encryption is claimed to be a vision of public key encryption that allows users to encrypt and decrypt messages based on users' attributes. In the scenario, users are represented by the summation of their attributes. An encryptor will associate encrypted data with a set of attributes. An authority will issue users different decryption keys, where a user's decryption key is associated with an access structure over attributes and reflects the access policy ascribed to the user. Notice that attribute-based encryption is a kind of one-to-many encryption.

Attribute based Encryption is a stochastic method that only takes the implied security parameter as input. The public parameters PK and a master key MK are the output parameters. Encryption: This is a stochastic algorithm with a message m, a collection of attributes γ and the public parameters PK as inputs. It generates the cipher text E as a result.

Key Generation: This is a stochastic algorithm that requires problems A, a master key MK, and public parameters PK as input. It generates D, which is a decryption key.

Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of resources. These computing resources can be rapidly provisioned and released with minimal effort. Cloud solutions come in three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The users communicate with the cloud through different modules like Ethernet, Wireless AP, Industry Switch, Access Network which are described as follows:

Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN). It enables devices to communicate with each other via a protocol, which is a set of rules or common network

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

language. A wireless access point (wireless AP) is a network device that transmits and receives data over a wireless local area network (WLAN), serving as the interconnection point between the WLAN and a fixed wire network.

A network switch connects devices in a network to each other, enabling them to talk by exchanging data packets. Switches can be hardware devices that manage physical networks or software-based virtual devices. Industrial switch has composable building blocks cloud services, applications, and other tools that are built for strategic use cases in specific industries. An access network is a user network that connects subscribers to a particular service provider and, through the carrier network, to other networks such as the Internet. Through these modules the user interacts with the cloud data.

Authentication and authorization are two vital information security processes that administrators use to protect systems and information. Authentication verifies the identity of a user or service, and authorization determines their access rights. It is possible to decrypt the data only with attributes which match recipients' attributes. Authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.

Decryption: The ciphertext E, which is encrypted using the set γ of attributes, the decryption key D for access control structure A and the public parameters PK are all inputs to this algorithm. If $\gamma \in A$, it outputs the message M.
The attribute based encryption makes the application to be secure. This approach provides better confidentiality and authenticity to cloud as it uses two different encryption techniques for key generation and data encryption and it provides double encryption to the data and it only decrypts the data whenever attributes are matched then only this system provides decrypted data.

## IV. RESULT ANALYSIS

In this section, Attribute Data Encryption and Decryption Technique For Cyber Security in Cloud Environment is implemented. The result analysis of presented approach is demonstrated here. The performance of presented approach is evaluated in terms of throughput, response time, Encryption Time and decryption time authenticity and confidentiality.

Encryption Time: The time required to encrypt data is termed as encryption time of the cryptographic system.

Decryption time: The time to recover original data from cipher is known as decryption time

Throughput: Throughput is the amount of the work a computer can do in a given period of time. It is a measure of comparative effectiveness of large computers that run programs concurrently.

Response Time: The amount of time between a single interactive user requests being entered and receiving the application's response is known as response time.

Authenticity: It is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Data confidentiality refers to protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information.

The fig. 2 shows the encryption time of presented approach.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

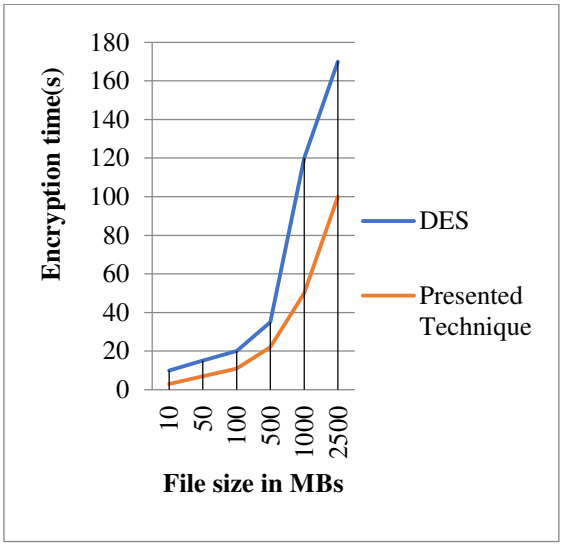


**Fig. 2: Encryption Time Comparison**

In fig. 2, the x-axis indicates the file size in MBs (Mega Bytes) and y-axis indicates the encryption time in seconds. Presented Attribute Data Encryption and Decryption Technique have required very less time for encryption than DES (Data Encryption Standard) approach. From Fig. 2, it is clear that the encryption time is increasing when the file size is increasing. The Fig. 3 shows the decryption time comparison. In fig. 2, the x-axis indicates the file size in MBs (Mega Bytes) and y-axis indicates the decryption time in seconds.

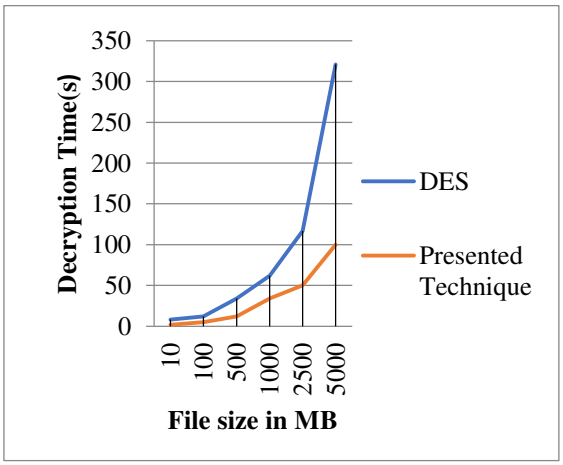


**Fig. 3: Decryption Time Comparison**

Compared to DES approach, presented approach has required less decryption time. The Table 1 shows the performance evaluation.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

**Table 1: Performance Evaluation**

| Performance Metrics | DES Algorithm | Attribute Data Encryption and Decryption Technique For Cyber Security in Cloud Environment |
|---|---|---|
| Response time (ms) | 60 | 10 |
| Throughput (%) | 72.12 | 95.23 |
| Authentication (%) | 75 | 97 |
| Confidentiality (%) | 80 | 97.23 |

Compared to DES algorithm, presented approach has better results in terms of throughput, authentication and confidentiality and very less response time. The Fig. 4 shows response time comparison. In fig.4, the x-axis shows the different approaches and y-axis indicates response time in ms. Compared to DES algorithm, presented Attribute Data Encryption and Decryption Technique has required less time to response.

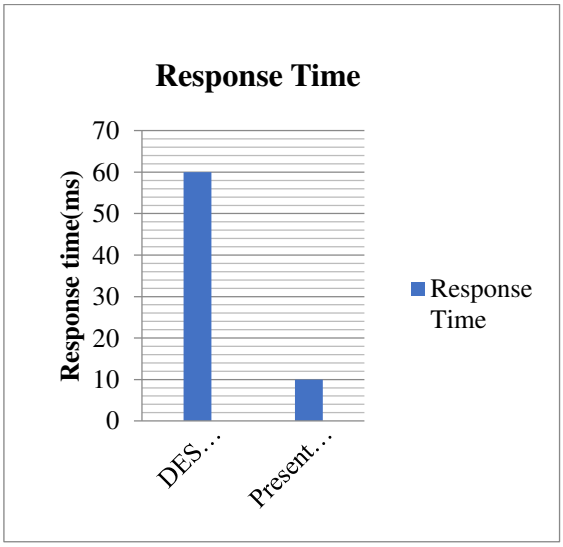


**Fig. 4: Response Time Comparison**

The fig. 5 shows the performance comparison in terms of throughput, authentication and confidentiality.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

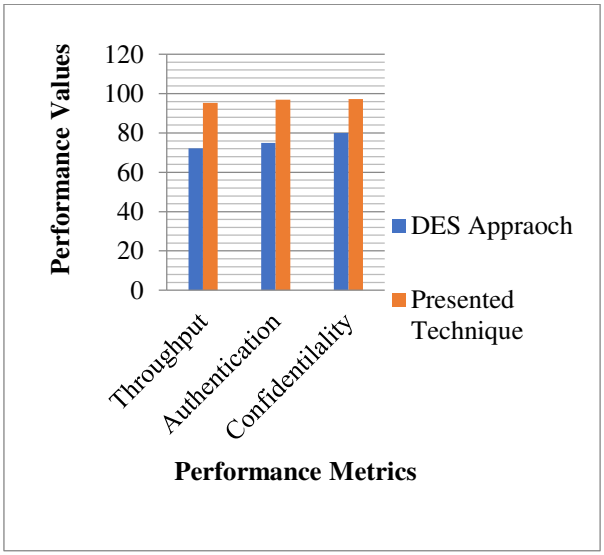


**Fig. 5: Performance Metrics Comparison**

Presented Attribute Data Encryption and Decryption Technique has high performance in terms of throughput, authentication and confidentiality than DES algorithm. Therefore presented encryption technique has shown significant results and provided better confidentiality and authentication to cloud data.

## V. CONCLUSION

In this work, Attribute Data Encryption and Decryption Technique for Cyber Security in Cloud Environment is presented. Security is very important feature for any technology. Using any technology will not be worth if it is not secure. RSA is used to generate Private key K. In this step the private key encryption is done to make the decoding of data more difficult. To encrypt the data Attribute data encryption and decryption technique is employed to encrypt and decrypt the data very securely. Attribute data encryption is a promising technique which has achieved flexible and fine-grained data access control over encrypted data, which is very suitable for secured data sharing environment in cloud computing environment. Authentication verified the identity of a user or service**,** and authorization determines their access rights. This technique decrypts the data only when the attributes are matched and then only authorization is provided to the user for decryption. The performance of presented technique is evaluated in terms of encryption time, decryption time, response time, throughput, authenticity and confidentiality. This technique has better results than earlier approach. In addition this technique requires less time for encryption, decryption and to response. This technique has provided greater authenticity, confidentiality and throughput. Hence, this technique is beneficial for secured data transfer and storing the data on cloud.

## REFERENCES

[1] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing", Inventive Communication and Computational Technologies, Lecture Notes in Networks and Systems 145, Springer, 2021, doi: 10.1007/978-981-15-7345-3_46

[2] B. Deepthi, G. Ramani, R. Deepika, Md Shabbeer. "Hybrid Secure Cloud Storage data based on improved Encryption Scheme", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), DOI: 10.1109/ESCI50559.2021.9396842

[3] Muhammad Usman Sana, Zhanli Li, Fawad Javaid, Hannan Bin Liaqat, Muhammad Usman Ali, "Enhanced Security in Cloud Computing Using Neural Network and Encryption", IEEE Access ( Volume: 9), 2021, DOI: 10.1109/ACCESS.2021.3122938

[4] Purvansh Jain, Piyush Muskara, Prati Jain, "Enhance Data Security in Cloud Computing with Digital Signature & Hybrid Cryptographic Algorithm", 2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM), DOI: 10.1109/SASM51857.2021.9841171

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 3, December 2021 ||

National Conference on Emerging Technologies [NCET' 2021]

Organized by

Royal College of Engineering and Technology, Thrissur, Kerala, India

[5] Pronika, S.S.Tyagi, "Secure Data Storage in Cloud using Encryption Algorithm", 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 978-1-6654-1960-4/20, 2021 IEEE, DOI: 10.1109/ICICV50876.2021.9388388

[6] Suresha D, Dr. K Karibasappa, "Enhancing Data Protection in Cloud Computing using Key Derivation based on Cryptographic Technique", Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC 2021) IEEE Xplore Part Number: CFP21K25-ART

[7] Md. Abu Musa and Md. Ashiq Mahmood, "Client-side Cryptography Based Security for Cloud Computing System", 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 978-1-7281-9537-7/20, 2021 IEEE, DOI: 10.1109/ICAIS50930.2021.9395890

[8] Yange Chen, Hequn Liu, Baocang Wang, Baljinnyam Sonompil, Yuan Ping and Zhili Zhang, "Yange Chen, Hequn Liu, Baocang Wang, Baljinnyam Sonompil, Yuan Ping and Zhili Zhang, "A threshold hybrid encryption method for integrity audit without trusted center Journal of Cloud Computing: Advances, Systems and Applications, 2021, doi: 10.1186/s13677-020-00222-6

[9] Omar Helmy Khafagy, Mohamed Hasan Ibrahim, Fatma A. Omara, "Hybrid-Key Stream Cipher Mechanism for HadoopDistributed File System Security", 2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE 2020), Aswan, Egypt, 2020, 978-1-7281-4801-4/20

[10] Srishti Bangera, Pallavi Billava, Prof. Sunita Naik, "A Hybrid Encryption Approach for Secured Authentication and Enhancement in Confidentiality of Data", Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020), IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2

[11] Zhenyong Zhang; Peng Cheng; Junfeng Wu; Jiming Chen, "Secure State Estimation Using Hybrid Homomorphic Encryption Scheme", IEEE Transactions on Control Systems Technology ( Volume: 29, Issue: 4, July 2020), DOI: 10.1109/TCST.2020.3019501

[12] Mustafa S. Abbas, Suadad S. Mahdi, Shahad A. Hussien "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography", 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Kurdistan Region – Iraq, 978-1-7281-5249-3/20, 2020 IEEE

[13] Avdhoot V. Mane1, Ankita Kumari, Aditi R. Mhaskar, Supriya P. Joshi, "Multimedia Security on Cloud Computing Using Cryptography", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 03, Mar 2020

[14] Shweta Kaushik, Ashish Patel, "Secure Cloud Data Using Hybrid Cryptographic Scheme", 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), DOI: 10.1109/IoT-SIU.2019.8777592

[15] Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE),7-9 February, 2019, 978-1-5386-9111-3/19

[16] Nadia Mohammed; Najla Ibrahim, "Implementation of New Secure Encryption Technique for Cloud Computing", 2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA), DOI: 10.1109/ICCISTA.2019.8830668

[17] Siddharth Singh, Varun Kumar, UtkarshVerma, Azhagiri M, "Data Security In Cloud Computing Using Cryptographic Algorithms", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 10 Oct 2019

[18] Kavita Saini; Vaibhav Agarwal; Arjun Varshney; Anushka Gupta, "E2EE for Data Security For Hybrid Cloud Services: A Novel Approach", **:** 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN),DOI: 10.1109/ICACCCN.2018.8748782

[19] Vishwanath S Mahalle; Aniket K Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm", 2014 International Conference on Power, Automation and Communication (INPAC),DOI: 10.1109/INPAC.2014.6981152

[20] Kamal Kumar Chauhan; Amit K.S. Sanger; Ajai Verma, "Homomorphic Encryption for Data Security in Cloud Computing", 2015 International Conference on Information Technology (ICIT), DOI: 10.1109/ICIT.2015.39

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com



Scan to save the contact details