ENHANCED DATA AUDITING AND AUTHENTICATION SCHEME IN CLOUD COMPUTING USING OUTSOURCED BAND MODEL

Miss Divya M. Kantode *SGBAU, Amravati Maharashtra, India.*

Dr. Mrs R.D. Raut *SGBAU, Amravati Maharashtra, India.*

Dr. V. M. Thakare *SGBAU, Amravati Maharashtra, India*

ABSTRACT

Nowadays, large amounts of data are stored with cloud service providers. Third-party auditors (TPAs), with the help of cryptography, are often used to verify this data. Auditing is the ability for cloud customers to verify the presence and functioning of their provider's security measures. Authentication is done by using username and password. The important point in authentication is to protect data from the access of unauthorized people. The proposed scheme is Enhanced RSA (ERSA) Algorithm. This paper presents solution to enhance the security and privacy to stored data in cloud. Result demonstrates that this scheme can improve the security of data that stored in cloud.

Index Terms — ***cloud computing; information security; confidentiality; integrity***

I) INTRODUCTION

Cloud computing is a service delivering mode based on the Internet. It can provide users with scalable services as required through the Internet and have been widely recognized and applied. To utilize computing resources more effectively and safely, people begin to pay close attention to hidden security problems in the Cloud. Access control is one of the most important measures to ensure the security of cloud computing. Cloud computing environment is a typical distributed environment; hence the distribution, dynamism, and anonymity of information resources and services are remarkable features of cloud computing environment [1].

The major technology used in cryptography is Encryption. This technology preserves confidentiality and integrity of data. The characteristic of confidentiality is data being made accessible only to authorized parties. Integrity will not allow unauthorized party to alter the data which is stored by the user. Many users acquire security by making their data very confidential Access control is one of the most important measures to ensure the security of cloud computing. Cloud computing environment is a typical distributed environment; hence the distribution, dynamism, and anonymity of information resources and services are remarkable features of cloud computing environment [2].

Cloud also allows the same technique towards the security concern. According to cloud environment, encrypting the users' data can be done by either two parties, namely, Third Party Auditor (TPA) or Cloud Service Providers (CSP) The two primary reason for growth in data storage in clouds are: a cloud-based storage system saves customers the overhead associated with the resources that would be necessary for a traditional in-house data storage solution, and instead, offloads these overheads to the cloud, and proliferation of capability constrained personal mobile computing devices[3].

Whenever the users rely on these parties, there is no reliability of data which is stored on cloud. A cloud service provider has an unlimited access to the data stored, and this aspect becomes especially important when public or hybrid clouds are used and the only thing users can rely on is decency of the provider. That is why confidentiality in cloud computing is an important security matter to both users and providers. The issue of trust to use of cloud resources, and to DCS in particular, is directly related to the issue of ensuring data security [4].

Thus, now-a-days the users themselves get into the process of encrypting their own sensitive data before sending it to cloud for storage. The **Enhanced RSA (ERSA) algorithm** uses two additional prime numbers in Standard RSA algorithm. This idea had been raised from High Speed and Security RSA algorithm which used two random numbers for key generation process. Using this proposed algorithms proposed method insures the confidentiality, integrity, availability and durability property of service which will improve the cloud services reliability [5].

This idea had been raised from High Speed and Security RSA algorithm which used two random numbers for key generation process. Using this proposed algorithms proposed method insures the confidentiality, integrity, availability and durability property of service which will improve the cloud services reliability.

II) BACKGROUND

The public system of auditing the security of the data stored in cloud computing and provided a privacy-preserving auditing protocol. It enables an external auditor to audit users cloud data without learning the content of the data. An efficient remote data auditing method for securing the storage of big data in cloud computing. In addition to third-party verification, dynamic operation, and other functions [1].

Trust computation mechanism will be introduced into access control model. Mutual trust between users and cloud service nodes are ensured through trust mechanism. Only trusted users have access to the Cloud, and simultaneously users can select the most credible cloud service nodes. The model had a good adaptability and malicious detection ability. In cloud computing environment, only when the security and reliability of both interaction parties are ensured, then the data security can be effectively interactions between users and the Cloud [2].

Storage systems with multiple data sources are highly relevant in several real world scenarios. The cloud storage service provider (CSSP) maintains a storage cloud providing the necessary infrastructure to create, store and update outsourced databases, and makes this data available to subscribing clients. The clients are given read-only access to the database, and authorized clients are allowed to make changes into the database [3].

In (DCS) Distributed Cloud Service provider has an unlimited access to the data stored, and this aspect becomes especially important when public or hybrid clouds are used and the only thing users can rely on is decency of the provider. Information stored in cloud computing is protected from faults of hardware. When using cloud computing, and distributed cloud storage (DCS) in particular, there arises some issues related to confidentiality and integrity of information in the process of both storage and transmission [4].

In RSA, an asymmetric key algorithm using two different keys for encryption and decryption processes. The Key size can be varied to make the encryption process strong. Hence it is difficult for the attackers to intrude the data. Increasing key size correspondingly increases the time taken for encryption and decryption process [5].

This paper introduces an enhanced data auditing and authentication scheme which helps to improve privacy of data owners this proposed theory. This paper organized as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing scheme. **Section V** analysis and discusses scheme results. **Section VI** proposed method. **Section VII** includes outcome result possible. **Section VIII** concludes this review paper. Section IX discusses Future Scope.

III) PREVIOUS WORK DONE

Guangjie Hanet.al (2016) [1] proposed a grid-based joint routing and charging algorithm for industrial wireless rechargeable sensor networks. TieQiu et.al [2016] proposed a greedy model with small world for improving the robustness of heterogeneous internet of things. Proposed framework uses a better load distribution strategy, which greatly reduces the computational overhead of the client. Proposed scheme includes an error response scheme, and results show that solution has good error-handling ability and offers lower overhead expenses for computation and communication than other approaches.

Lei et al. (2013) [2] proposed Trust Based Access Control Policy in Multi-Domain of Cloud Computing. The proposed method combining with Trust Management (TM), a mutual trust based access control (MTBAC) model. MTBAC model take both user's behaviour trust and cloud Services node's credibility into consideration. Trust relationships between users and cloud Service nodes are established by mutual trust mechanism. Security problems of access Control are solved by implementing MTBAC model into cloud computing environment. Simulation experiments show that MTBAC model can guarantee the interaction between users and cloud service nodes.

Liu et al. (2015) [3] proposed Auditing for data integrity and reliability in cloud storage. The proposed present a query authentication scheme for cloud-based storage system where the data is populated by multiple sources and retrieved by the clients. The system allows clients to verify the authenticity and integrity of the retrieved data in a scalable and efficient way, without requiring implicit trust on the storage service provider. The proposed mechanism is based on recently proposed multi-trapdoor hash functions, using its properties to achieve near constant communication and computation overhead for authenticating query responses, regardless of the data size, or the number of sources.

GuoW.et.al (2014) [4] proposed insights into the advancements of enterprise cloud. Proposed methods of encrypted data handling include four key elements, such as an agent, a controller, an auditor and a DCS. The agent is installed on client’s hardware and contains all procedures of saving, reading, deleting, encrypting and decrypting of data, as well as requests for authentication and authorization for accessing a DCS and algorithms of client’s data encryption and sending data to nodes within the DCS. The controller is responsible for storing information about files in a database and contains procedures of receiving tokens and data distribution to nodes within the DCS, and authentication and authorization procedure using the auditor.

Vishwanath S. Mahalleet.al (2016) [5] proposed method for enhancing the data security in Cloud by implementing Hybrid (Rsa&Aes) Encryption Algorithm. Encryption is done by using any one of the popular symmetric or asymmetric key algorithms such as AES, DES, RSA, Blowfish and Triple DES etc., RSA algorithm which is a asymmetric key algorithm using two different keys for encryption and decryption processes. The Key size can be varied to make the encryption process strong. Hence it is difficult for the attackers to intrude the data. Increasing key size correspondingly increases the time taken for encryption and decryption process. The proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size. This strength paves the way to store data in cloud by the users without any inconvenience.

IV) EXISTING METHODOLOGIES

A. An Efficient Protocol with Bidirectional Verification

Proposed auditing protocol support dynamic data operations, which is efficient and has been analysed to be secure in the random oracle model. Proposed auditing protocol provides the support for bidirectional authentication and statistical analysis. The public system of auditing the security of the data stored in cloud computing and provide privacy-preserving auditing protocol.

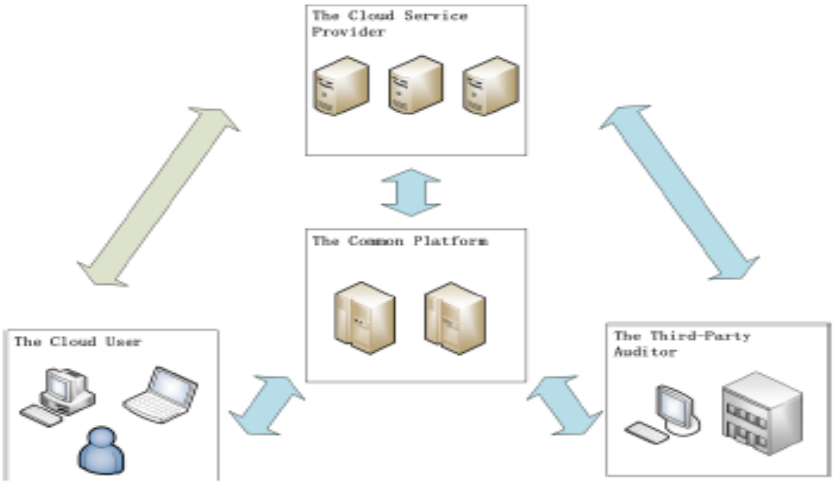

Fig. 1, System model

Proposed scheme enables an external auditor to audit users cloud data without learning the content of the data. In order to make processing more efficient, the calculations of the client account for only a very small part of the total amount of calculation. When the file is changed, the data owner can check to determine whether the important parts are in good condition. Further, the data owner can roughly determine the location of the error, thereby protecting the data that has not been changed.

B. A Mutual Trust Based Access Control Model

The proposed method will be introduced trust computation mechanism into access control model. Mutual trust between users and cloud service nodes are ensured through trust mechanism. MTBAC model not only considers user's behaviour trust and ensure that user's access request poses no malicious threat to cloud server, and also takes cloud service node's credibility into account.

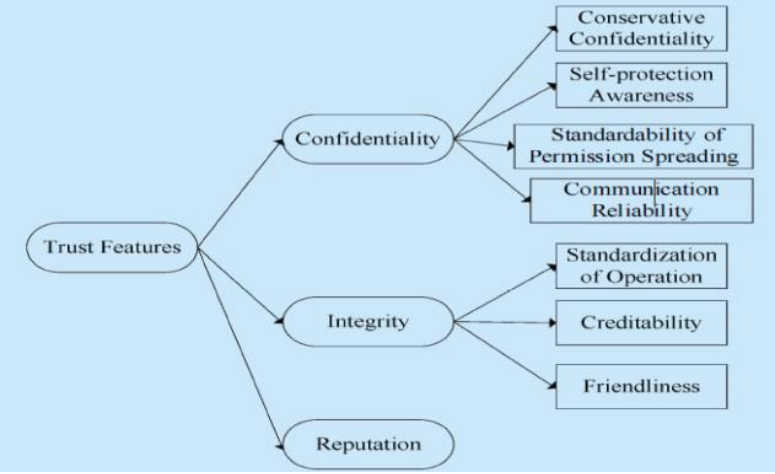

Fig. 2, the Division of Trust Attribute

The mutual trust mechanism of users and cloud service nodes has a two-part structure. One part is trust evaluation model of users' behaviour and the other part is trust computation model towards cloud service nodes. The network level, made up of three attributes, confidentiality, integrity and reputation; the bottom is composed of data items of trust attributes. Confidentiality includes conservative confidentiality. User's behaviour trust is the comprehensive evaluation and prediction from cloud server. Each kind of trust attribute has different impact on user's overall behaviour trust values, therefore, it need to quantify the qualitative and fuzzy influences accurately, and then acquire the exact trust values.

C. Efficient and Scalable Query Authentication with Multiple Data Sources

The proposed method present a novel mechanism for authentication of query results in a cloud-based storage system with support for multiple sources that achieves constant communication and computation overheads regardless of the data size, or the number of sources. The proposed scheme achieves this by generating authentication tags of individual data elements and aggregating tags of multiple data elements using a novel mechanism based on the recently proposed paradigm called a multitrap door hashing scheme.

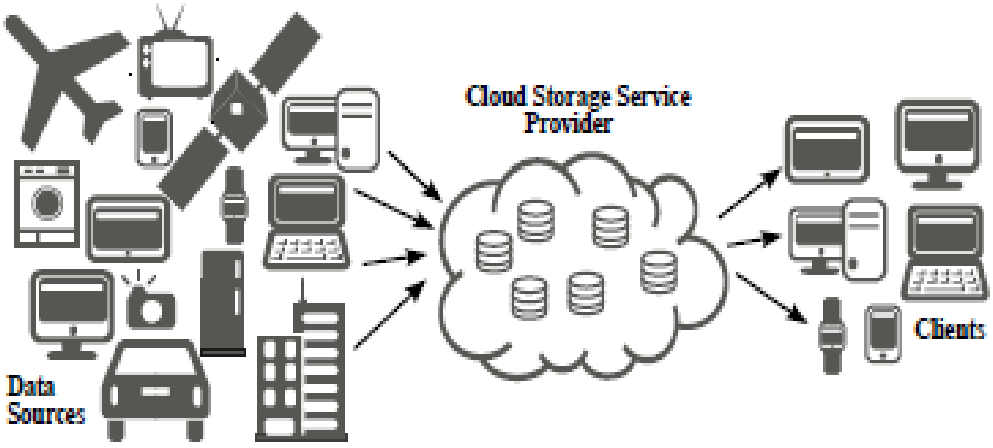

Fig. 3, Cloud based storage system

Query authentication scheme for multi-source cloud-based storage systems to provide light weight operation and high security. In terms of operational costs, aim is to minimize the storage, computation

and communication overhead at each entity, using cryptographic techniques that scale with the number of data sources, and sizes of the database and query response.

D. The Method of Ensuring Confidentiality and Integrity Data

A method that describes the use of separate services outside the cloud for authentication, data management and metadata storage to eliminate the possibility of obtaining unauthorized access to data, and the use of metadata to perform integrity control. The owner of the database limits the access to data that is stored in an encrypted form and does not allow provider to interact with database.

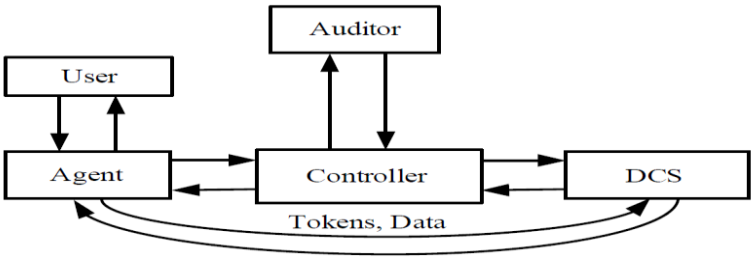

Fig. 4, Methods of encrypted data handling

Proposed a system of storage and generation of metadata based on checksums of information and time is introduced. Proposed method derived the set of methods of encrypted data handling in DCS that develop consists of procedures of saving, receiving and deleting data from DCS. All operations with encrypted data carried out in cloud computing should be performed without decryption. It is essential to store encryption keys beyond cloud computing.

E. E. Enhanced RSA Algorithm with varying Key Sizes for Data Security

The major technology used in cryptography is Encryption. This technology preserves confidentiality and integrity of data. The characteristic of confidentiality is data being made accessible only to authorized parties. Integrity will not allow unauthorized party to alter the data which is stored by the user. Many users acquire security by making their data very confidential.

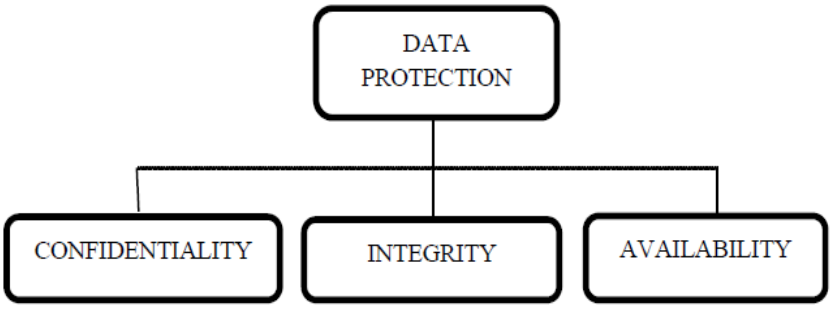

Fig. 5, Data protection method

Encryption is done by using any one of the popular symmetric or asymmetric key algorithms such as AES, DES, RSA, Blowfish and Triple DES etc., RSA algorithm which is a asymmetric key algorithm using two different keys for encryption and decryption processes. The Key size can be varied to make the encryption process strong. Hence it is difficult for the attackers to intrude the data. Increasing key size correspondingly increases the time taken for encryption and decryption process. The proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size. This strength paves the way to store data in cloud by the users without any inconvenience.

V) ANALYSIS AND DISCUSSION

The auditing protocol support dynamic data operations, which is efficient and has been analysed to be secure in the random oracle model. Proposed auditing protocol provides the support for bidirectional authentication and statistical analysis [1].

Access control is one of the most important measures to ensure the security of cloud computing. Mutual trust between users and cloud service nodes are ensured through trust mechanism. Only trusted users have access to the Cloud, and simultaneously users can select the most credible cloud service nodes [2].

A novel mechanism for authentication of query results in a cloud-based storage system with support for multiple sources that achieves constant communication and computation overheads regardless of the data size, or the number of sources [3].

When using cloud computing, and distributed cloud storage (DCS) in particular, there arises a range of topical issues related to confidentiality and integrity of information in the process of both storage and transmission. Some separate services outside the cloud for authentication, data management and metadata storage to eliminate the possibility of obtaining unauthorized access to data, and the use of metadata to perform integrity control. [4].

The conventional security mechanism in the normal network is Cryptography. It plays a major role in the security concern. The major technology used in cryptography is Encryption. This technology preserves confidentiality and integrity of data. The characteristic of confidentiality is data being made accessible only to authorized parties. Integrity will not allow unauthorized party to alter the data which is stored by the user [5].

Existing Methodologies	Advantages	Disadvantages
Efficient protocol with bidirectional verification	When the file is changed, the data owner can determine the location of error, thereby the given data has not been changed.	The data auditing methods assume that the data owner's secret key is secure. But, in fact, this is not necessarily correct.
Mutual Trust based access control	Access control in cloud computing environment on the basis of the mutual trust between users and the cloud service nodes.	The access control mechanism does not apply to large-scale, distributed network.
Efficient and Scalable Query Authentic ion Authentication with Multiple Data Sources	It can be achieves constant communication and computation overheads regardless of the data size, or the number of sources.	Other limitations include lack of public verifiability, fixed number of verifications, and high cost of updates.

Ensuring Confidentiality and Integrity Data	Information stored in cloud computing is protected from faults of hardware.	Methods of ensuring confidentiality that are in use at the moment are ineffective for cloud computing
Enhanced RSA Algorithm with varying Key Sizes for Data Security	The usage of prime numbers instead of random numbers it improves the speed of encryption and decryption	The users rely on other parties; there is no reliability of data which is stored on cloud.

Table1: Pro and Cons of existing methodologies.

VI) PROPOSED METHODOLOGY

First, Proposed Methodology proposes schemes which will helps to enhance security and authentication in cloud services. Proposed method introduce encryption and description scheme which eventually improves authentication process. First user login if user exists otherwise first user registration by using registration form. After the successful completion of login process then user can himself get the authority for storing the data into the cloud. Authorized user can select the two random picture or image from the gallery then form the one new image from these two images and this one new image is called as image fusion because this new image is a combination of these two images. Image fusion uses the numbers of XOR keys then user can select the random XOR key number. From these keys one strong password is generated and using this password, the user can select required data those are placed into the cloud. So that user can select maximum data for storing into the cloud and also achieve the security for stored data.

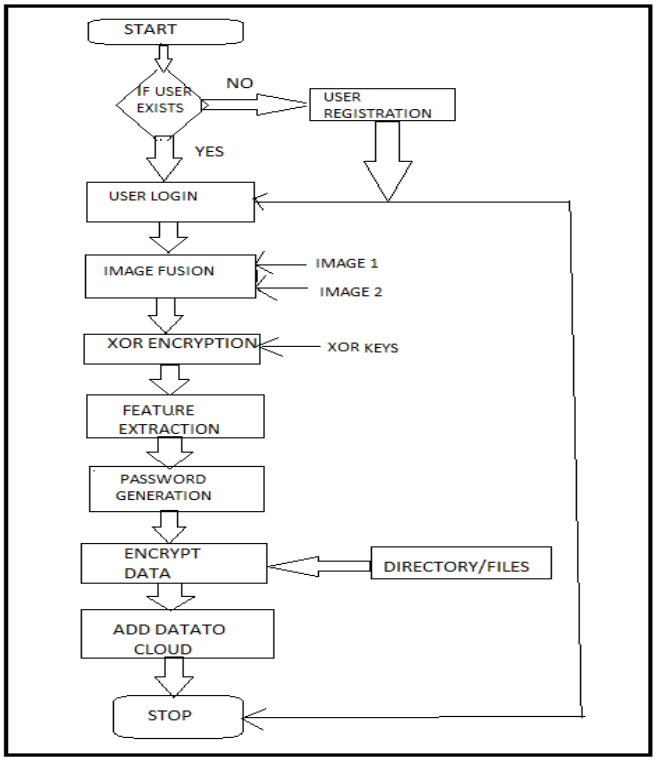

Fig.1, Data Encryption

Second, Proposed methodology added secure encoding which helps to permit authenticated access and also restrict the unwanted access. Registered user generates secure login credentials which can be utilize each time when user accesses cloud services, this secure login prevents system from cloud attackers. The below diagram of Data Decryption describes the working of proposed framework. The Registered user can first load the file those are removing from the cloud then select the specific folder or image or document. After successful selection then decrypt this data and save this decrypted data into specific location or path.

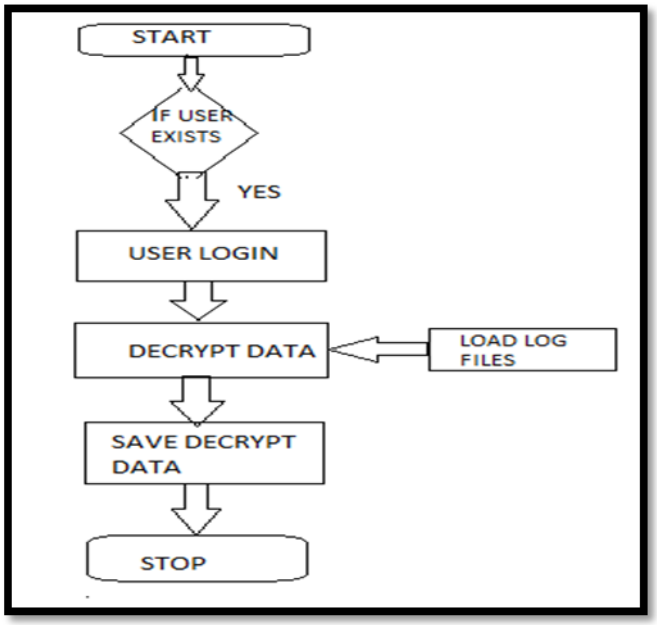

Fig.2, Data Decryption

VII) OUTCOME AND POSSIBLE RESULT

This paper proposes an improvement regarding encryption and decryption time. The Encryption and Decryption time for High Speed and Secure RSA algorithm and the proposed algorithm ERSA are taken into consideration for better performance. It is highly scalable in terms of computation and communication overheads regardless of the data size, or the number of sources. Thus, overall, the proposed scheme achieves superior scalability and efficiency.

VIII) CONCLUSION

This paper focused on the speed is still enhanced in the proposed algorithm ERSA by dividing the file into several blocks. Apart from increasing the speed, the implementation of ERSA algorithm also makes the computation complex one and increases the strength of security. The result demonstrates that the reduction in encryption and decryption time according to ERSA than the High Speed and Secure RSA.

IX) FUTURE SCOPE:

In this paper proposed scheme only ensures the authenticity and integrity of selection query results. In future plan to extend this mechanism to also provide completeness guarantees, which will allow the client to verify that the cloud, returns every file that satisfies the query condition, support different types of queries.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith et al., ”A view of cloud computing,” Communications of the ACM, 2013, vol.53, no.4, pp. 50-58.
[2] Guoyuan Lin, Yuyu Bie, Min Lei. Trust Based Access Control Policy in Multi-Domain of Cloud Computing. IEEE Journal 2013, pp. 1357-1365.
[3] J. Yuan and S. Yu, “Efficient public integrity checking for cloud data sharing with multi-user modification,” in *Proceedings of INFOCOM, IEEE Conference on Computer Communications, Toronto, Canada, April 27 - May 2*. IEEE, 2014, pp. 2121–2129.
[4] Boyen X. General Ad Hoc Encryption from Exponent Inversion IBE. EUROCRYPT 2015. V. 4515. P. 394–411.
[5]Vishwanath S. Mahalle, Aniket K. Shahade, “Enhancing the data security in Cloud by implementing Hybrid Encryption Algorithm”, IEEE, 2016, pp. 146-149.