Comparative Analysis of Various Cloud Security Frameworks

Ashima Narang[a], Dr. Deepali Gupta[b]
a. PhD Scholar, Computer Science Department, Maharishi Markandeshwar University, Sadopur, Ambala, India
b. Professor & head, Computer Science Department, Maharishi Markandeshwar University, Sadopur, Ambala, India

Abstract: Cloud is one of the technologies, the use of which will be increases day by day for different purposes as per user's requirement. Mostly this technology is used for storage purpose as because of this the users need not to have any hardware storage devices instead of that their data will be stored on the network. These systems have to be more secure so that they provide confidentiality, privacy and protection for their customer's satisfaction. Various algorithms were developed to secure cloud frameworks but still these algorithms are not able to meet the requirements of the users. To find out the lack, a comparison of existing security architectures will be covered in this paper where we will consider three different security architectures and will compare these on the basis of Computation Time (for both encryption and decryption), Computation Cost (for both encryption and decryption), and Cipher Text Size.

***Index Terms*—Cloud computing, Cloud Security, key management, blowfish, HASBE, encryption, Diffie Hellman, RSA, ECC**

1. INTRODUCTION

In this fast paced life, people are now very much inclined to the technology and the world will become more tech savvy as compare to former timings and in this time, cloud has been one of the favorite technical paradigm in the field of computation and provides a various services as required by users which includes software resources as well as hardware resources from distinct data centers using Internet to fulfil the demands of their clients.

The numbers of services are provided by cloud models that includes software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) as per the necessity of the users. These service models are isolated with their segregated functions and the liabilities of these are under hazardous situations. So, there is a need to protect cloud infrastructure and it is one of the important concern as its usage will be increasing day by day. There are different security mechanisms were proposed by many researchers but these techniques are not able assure that the cloud is now risk free. For instance, the main focus of the traditional security algorithms was either to provide a protective shield to the data that user wants to store or to cater proof for the validation of the users by using distinct mechanisms which does not address the security issues so, nowadays a secure system is required which will highly focus on the security parameters and also need to collaborate authentication and data privacy for the immense level of security, and for this, need to take care of the entire aspects of the cloud either from user end or service end.

Moreover, cloud becomes the key ingredient for the most of the business organizations which help to the reduction of the storage space for the load of abundant data as that can be hold by the cloud. These days, even an ordinary users are strongly influenced by the features of the cloud like dedicated storage facilities so they are keen to use it. However, this increased demand will be the main cause of the insecurity of the data.

Cloud security paradigm includes set of policies and technologies that heed to protect cloud system and its data from forgeries. Various data protection and security techniques have been proposed by different researchers that focussed to gain the user's interest by providing assurance of the security. Like, cloud based privacy manager [18] which preserves the privacy of the cloud but there is a requirement of the honest service providers. The other existing methods are Anonymity based methods [19], Public Auditability and data Dynamics for Storage Security [22], Privacy-Preserved Access Control [25], Fog Computing [27], Security using Elliptic Curve Cryptography [29], and Fully Homomorphic Encryption [20]. However, these techniques need to be analyzed and also need to improve for future usage of the cloud.

From the previous concept of deployment models, cloud computing [1] is gaining the popularity. These days, several companies, big enterprises, are enjoying the comforts of cloud services and putting their applications and data into it. This results in more efficiency and effectiveness in developing and deployment and the burden of purchasing and maintaining the infrastructure is no more a requirement. One of the most useful and widely used definition of cloud is NIST as "Cloud computing is a technique that allow convenient, according to users requirement provides network access to computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly allocated and released with least management work. The cloud model consists of five characteristics, three services, and four deployment models."[2] The three service models of cloud are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud.

Furthermore, the issue of the security are under consideration as cloud still faces the challenges in terms of protection of data as well as falsification and these can also be deviate because of the type of the data. The main objective of this paper is to analyze latest solutions and find out which one will be more effective to handle the upcoming challenges of cloud computing. The next sections of this paper describe three different existed solutions for the protection of different type of data with complete analysis on the basis of different factors. These solutions are one of the latest security mechanisms that highly cure the cloud system from intrusions.

2. A Practical Group Key Management Algorithm

The main focus of this algorithm is to develop a secure mechanism for cloud computing using practical group key management algorithm. In this architecture user use the services of sharing data with each other [ ]. This algorithm provides two level encryption using Computational Diffie-Hellman Algorithm.

2.1 Architecture of the Cloud Data Sharing System

In this work, Data sharing system consists of a cloud users, storage server and data owner. Users in this cloud are both authenticated and non-authenticated. Data can be stored to the cloud server by data owners and then they can share it with different authorized users with whom they want to. There are several groups of these authorized users and shared data was authorized to all he groups. Data is accessed by the users of the authorized group only at the cloud server. The data owner uploads their data to cloud server but for the protection of data, owner firstly encrypt it. This model is not fully trusted to evaluate the performance of the security mechanisms which was design to detect the intruders and provide secure communication between different users.

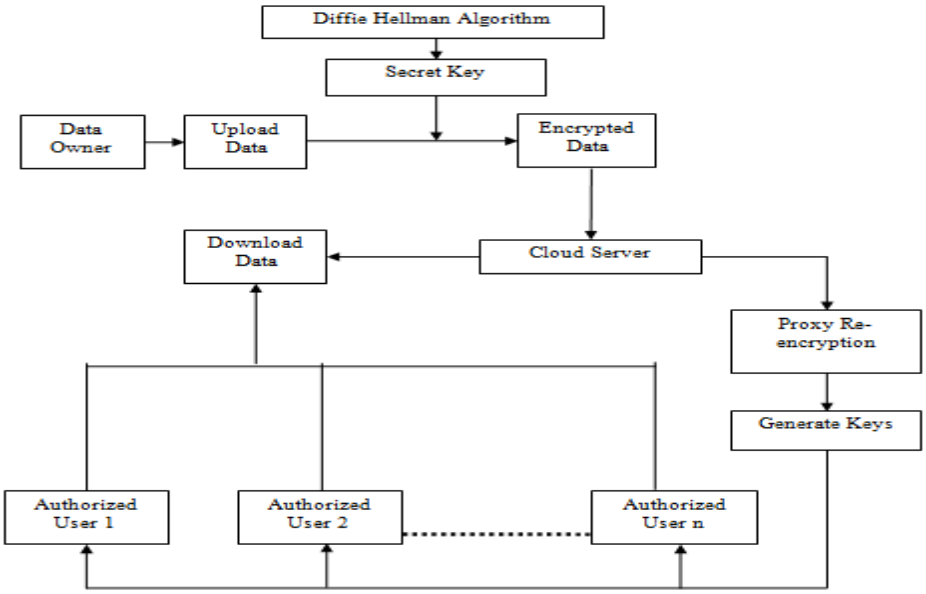

Fig 1. Practical Group Key Management Algorithm

In this architecture there are three main entities that are: (i) Cloud Users, (ii) Cloud Servers, and (iii) Data Owners. In this, firstly data is uploaded to the cloud server by its owner to distribute it to other cloud users. This data is firstly encrypted using secret key generated using Diffie-Hellman algorithm. This data is not only meant to use by the owner but also other authorized users access it. Storage services are provided by the cloud server where cloud server imitates the process of the proxy to distribute keys and generate it using re-encryption mechanism. On the other hand, other users of the cloud can access the data authorized by the owner and they have the key which will be used to decrypt data.

2.2 Key Generation Algorithm

In this work, Secret key is generated using Diffie-Hellman algorithm which is used to encrypt data but for data sharing, proxy re-encryption mechanism [ ] is used which includes the following steps:

(i) Generate Random Number,
(ii) Key Generation,
(iii) Re-encryption key generation,
(iv) First-level encryption,
(v) Second-level encryption.

2.3 Group Key Management

The group key mechanism is based on two layer mechanism where first layer is group layer and other is user layer. Six polynomial algorithms are used in this mechanism these are: initialization, key generation, add group users, authorization and revocation [].

3. Data Encryption using HASBE and Blowfish

In this work, Hybrid combination of two encryption algorithms Hierarchical Attribute Set Based Encryption and Blowfish Algorithm were implemented. The main focus of this is to provide a secure and efficient delivery of the data.

3.1 Description

In this, a new technique is generated by smearing cloud with existing encryption mechanisms and check about the warehousing of the documents in cloud. This can be achieved by the combination of hierarchical attribute set based encryption and blowfish algorithm with service level agreement. Data redundancy is decreased by compression. The main weakness of the current encryption algorithms is the time to broadcast it, time taken by the algorithm to encrypt the data and redundancy as well. With the advancement in the hardware technologies, plenty of researches are going on for the up-gradation of the transmission of the data. The data size gets reduced due to compression and their transmission is quite faster than the original data. Encryption is must to ensure the communication risk free. Data need to be encrypted before transmit/upload it to the server.

3.2 Methodology

In this, when user uploads their data to the cloud server, it first encrypted with the key which is generated using hybrid algorithm as shown in figure. This hybrid algorithm [ ]is a combination of hierarchical attribute based encryption (HABE) and blowfish algorithm where HASBE is an extended version of Attribute based encryption (ABE) to deal with the hierarchical structure of the system users. In HABE [3], encryption is not done only from one particular user as it was done in earlier cryptography algorithms. Instead of that, keys are associated with set of policies or attributes and a user can decrypt the data only if it is matched with the ciphertext and decryption key. Blowfish generates a variable length key to encrypt the data before uploading on the server.

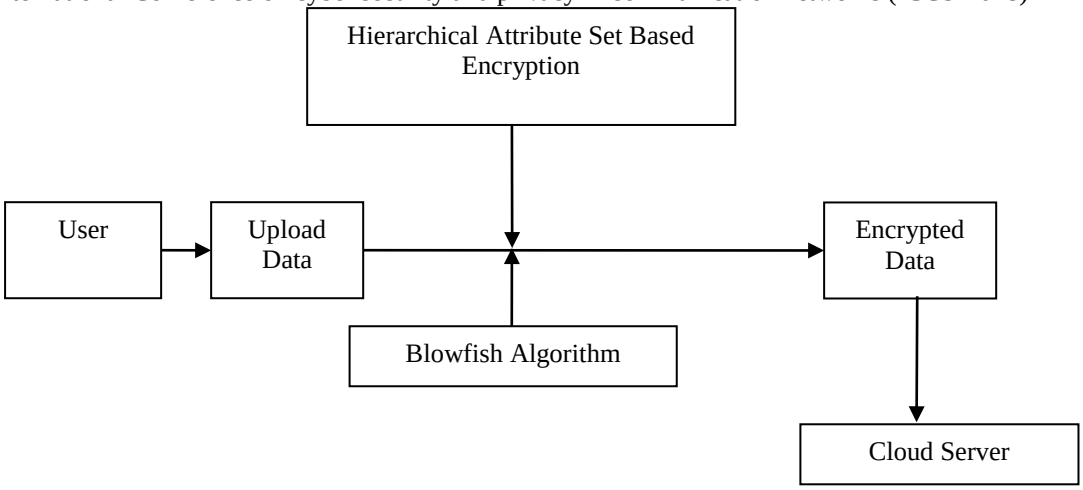

Fig 2. Hybrid HBASE & Blowfish Algorithm

4. Keyword Encryption and Hybrid Cryptographic Algorithm

In this, a novel identity based hybrid encryption (RSA with ECC) to enhance the security of outsourced data was proposed. In this approach sender encrypts the sensitive data using hybrid algorithm. Then the proxy re encryption is used to encrypt the keyword and identity in standardize toward enrichment security of data.

4.1 Methodology

In this hybrid algorithm, Data is encrypted at the sender side using identity of the receiver (ID) which further used for two different purposes one is added to the receiver identity's encryption and the other is used as a keyword for ciphertext generation. To encrypt keyword and receiver's identity, Proxy re-encryption is used in this approach. Different tags are used as keywords for example, secret or top secret and many more.

In this, when a message Ms sent by a user to the receiver with keyword Kw, E(IDa,Ms)|| PRE(IDa,Kw) sent to the server. Decryption will be done on the receiver side only by using its own decryption key which depends on the identity of user and PKG provides that key. Like in figure , it is very clear that whenever user upload their data, the data has been encrypted before uploading on the server using hybrid RSA & ECC algorithm.

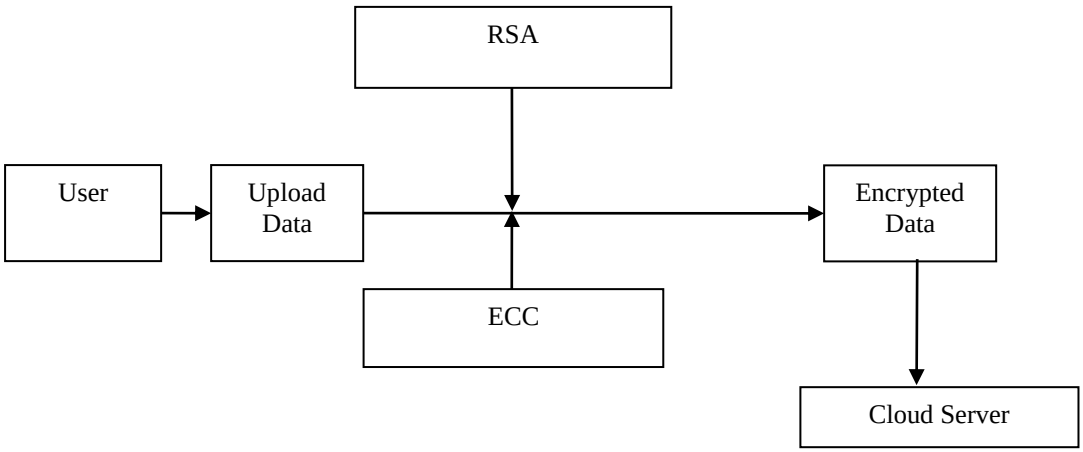

Fig 3. Hybrid RSA & ECC Algorithm

5. Results Analysis

To compare and analyze the performance of different security methods in cloud computing different parameters are used. These are:

Time Analysis: Time can be measured for storing each file on server. Here Time can be defined as a time taken to store data on the server. Also total time can be calculated by adding the time of all files that are stored on the server. Total time can be calculated as :

$$Total\ time\ (T_{Total}) = \sum_{i=0}^{n} T_i$$

Testing has been done for these three methods on a dataset of 20 files. Where 15 text files and 5 image files has been uploaded to the cloud environment with three different methods and Total Time for storing data on server is as given in table:

Table 1: Total Time (in sec)

	Diffie Hellman + Reencryption	RSA+ECC	Blowfish+ Attribute Based Encryption
Total Time	46.44	38.34	40.62

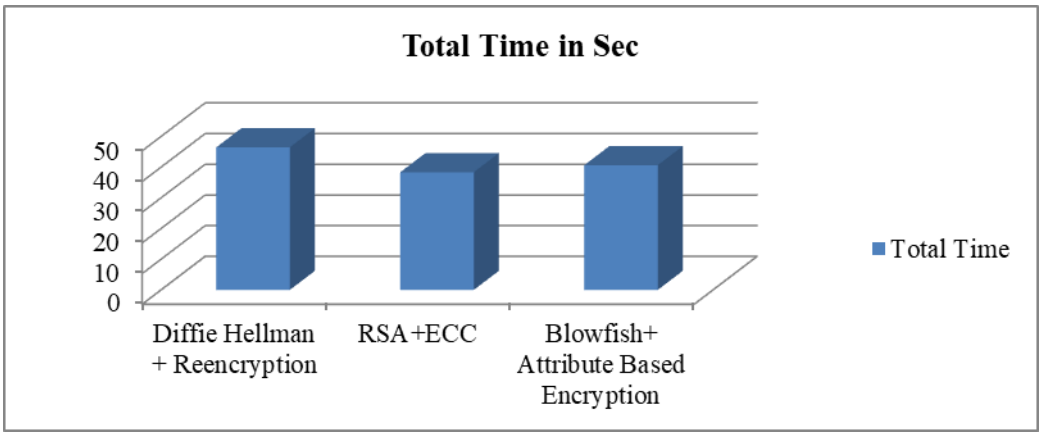

Fig 4. Results of Algorithms-Total Time

According to analysis, Storage time of hybrid RSA & ECC is lesser than others so it is better in terms of time

Throughput Analysis : Scalability of the framework can also be measured by calculating throughput of the framework. Here throughput can be defined as rate of transactions don in a given time. It can be calculated as:

$$Throughput = \frac{Total\ no.of\ files}{Total\ Time} * 100$$

Testing has been done for these three methods on a dataset of 20 files. Where 15 text files and 5 image files has been uploaded to the cloud environment with three different methods and Throughput for this data on server is as given in table:

Table 2: Throughput (in %)

	Diffie Hellman + Reencryption	RSA+ECC	Blowfish+ Attribute Based Encryption
Throughput	43.07	52.15	49.24

Method-1,

$$Throughput = \frac{20}{46.44} * 100 = 43.07\%$$

Method-2,

$$Throughput = \frac{20}{38.34} * 100 = 52.15\%$$

Method-3,

$$Throughput = \frac{20}{40.62} * 100 = 49.24\%$$

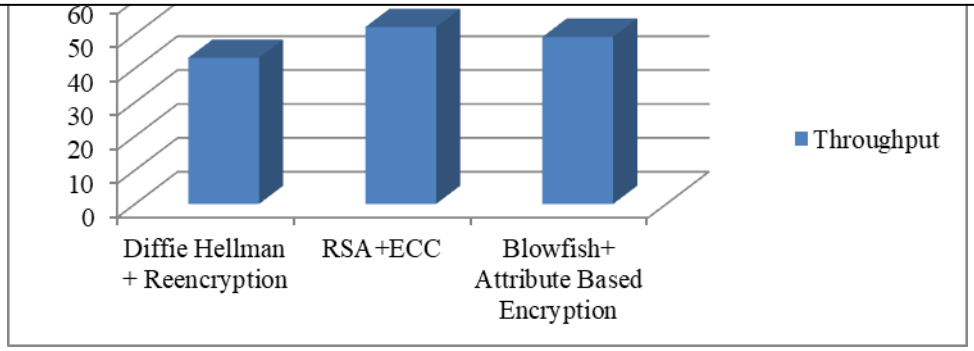

Fig 5. Results of Algorithms-Throughput

It is analyzed that, Throughput of hybrid RSA and ECC is greater than others so it is better in terms of throughput also.

Size: In this size of the data after encryption is calculated and compared. Testing has been done for these three methods on a dataset of 20 files. Where 15 text files and 5 image files has been uploaded to the cloud environment with three different methods and Original size of data is 5838KB. The size after encryption is:

Table 3: Size (in KB)

	Diffie Hellman + Reencryption	RSA+ECC	Blowfish+ Attribute Based Encryption
Size	5838	5839	22223

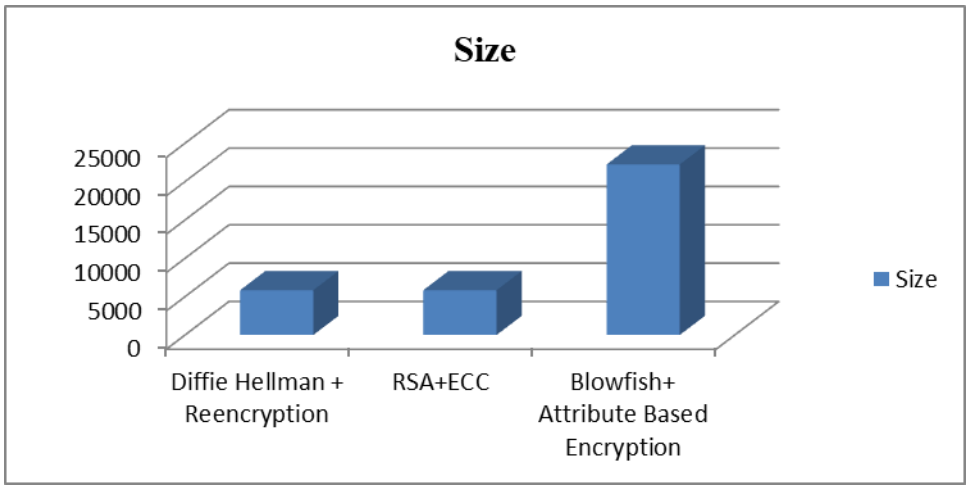

Fig 6. Results of Algorithms-Size

Size of data after encryption is almost same as original for both **Practical Group Key Management Algorithm** and hybrid RSA-ECC. This means encryption doesn't affect more on data whereas in hybrid HABE-blowfish the size of data is increased.

6. Conclusion

Cloud computing will be the most prior are of the technology whose demand will increase day by day and it needs to be very efficient for providing services to their users with high efficiency and privacy. So the main focus of this paper was to analyze the current state of the security in cloud computing where analysis of the three recent security technologies were done. In this analysis, diffie hellman based approach, hybrid HBASE and Blowfish, and hybrid RSA & ECC were used and experimentation was done for the same by implementing these algorithms and generating architecture similar to the literature with these three algorithm. For analysis, text files and image files were uploaded to the server and different parameters were examined that includes, time, throughput, and size of the data after encryption. Results show that hybrid RSA & ECC outperform from the other methods. So this can be further considered for enhancement or to provide more secure environment to the cloud server.

REFERENCES

[1]. W. Song, H. Zou, H. Liu, and J. Chen, "A practical group key management algorithm for cloud data sharing with dynamic group," China Communications, vol. 13, no. 6, pp. 205–216, 2016.

[2]. N. Jayapandian, A. Z. Rahman, R. Sangavee, and R. Divya, "Improved cloud security trust on client side data encryption using HASBE and Blowfish," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), pp. 1–6, 2016.

[3]. G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3688–3693, 2016.

[4]. Z. Wan, J. Liu, and R. H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

[5]. M. Mowbray and S. Pearson, "A client-based privacy manager for cloud computing," Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE - COMSWARE 09, 2009.

[6]. J. Wang, Y. Zhao," Providing Privacy preserving in cloud computing," International Conference on Test and Measurement," vol. 2, pp. 213–216,2009.

[7]. C. Gentry.," Fully Homomorphic encryption using ideal lattices.," STOC, pp. 169–178, 2009.

[8]. A. Squicciarini, S. Sundareswaran, and D. Lin," Preventing Information Leakage from Indexing in the Cloud," 2010 IEEE 3rd International Conference on Cloud Computing, pp. 188–195,2010.

[9]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

[10]. R. Mishra, D. P. Mishra, A. Tripathy, and S. K. Dash, "A privacy preserving repository for securing data across the cloud," 2011 3rd International Conference on Electronics Computer Technology, vol. 5, pp. 6–10, 2011.

[11]. U. Greveler, B. Justus, and D. Loehr, "A Privacy Preserving System for Cloud Computing," 2011 IEEE 11th International Conference on Computer and Information Technology, pp. 648–653, 2011.

[12]. M. Zhou, Y. Mu, W. Susilo, M. H. Au, and J. Yan, "Privacy-Preserved Access Control for Cloud Computing," 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 83–90, 2011.

[13]. J. Singh, B. Kumar, and A. Khatri, "Improving stored data security in Cloud using Rc5 algorithm," 2012 Nirma University International Conference on Engineering (NUiCONE), pp. 1–5, 2012.

[14]. S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," 2012 IEEE Symposium on Security and Privacy Workshops, pp. 125–128, 2012.

[15]. Y. Brun and N. Medvidovic, "Keeping Data Private while Computing in the Cloud," 2012 IEEE Fifth International Conference on Cloud Computing, pp. 285–294, 2012.

[16]. V. Gampala,S. Inuganti, S.Muppidi, "Enhancing Data Security Using Elliptic Curve Cryptography in Cloud Computing," International Journal of Science and Research (IJSR), vol. 5, no. 7, pp. 1884–1890, May 2016.

[17]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," 2010 Proceedings IEEE INFOCOM, pp. 1–9, 2010.

[18]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[19]. X. Li, J. He, T. Zhang," A Service Oriented Identity Authentication Privacy Protection Method in Cloud computing," International Journal of Grid and Distributed Computing,vol. 6, no. 1, 2013

[20]. Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks, vol. 10, no. 7, pp. 1–9, 2014.

[21]. C.-Y. Chen and J.-F. Tu, "A Novel Cloud Computing Algorithm of Security and Privacy," Mathematical Problems in Engineering, vol. 2013, pp. 1–6, 2013.

[22]. Y. Yang, X. Chen, H. Chen, and X. Du, "Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing," IEEE Access, vol. 6, pp. 18009–18021, 2018.

[23]. S. Ashraf, T. Kehkashan, M. Gull, and S. M. U. Din, "Transparency service model for data security in cloud computing," 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pp. 1–6, 2018.

[24]. B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, and T. Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," IEEE Access, vol. 4, pp. 7899–7911, 2016.