A Survey on Security in Cloud Computing

S. Sasirekha[1], M. Usharani[2]

[1]Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India, rehasenthil@gmail.com.

[2]PG Scholar, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India, musharani28cse@gmail.com.

Abstract - Cloud computing is one of the best ever growing internet based expertise that facilitates users to utilize services by making use of large poll of resources without installation of any software. Adoption of this technology is increasing because of many advantages including reduction of cost and IT load. Regardless of the recognition of cloud computing, it faces many difficulties such as security that is one of the major inhibitors in the growth of cloud computing. The security of cloud computing plays a vital role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. The main issue of cloud storage is to secure the data. Many of the security algorithms are available in the cloud computing environment. Encryption is one of the widely used methods to ensure the data confidentiality in cloud environment. In this paper, we will discuss the different techniques that are used for secure data on cloud.

Keywords - Cloud computing, Cloud data security, Data Encryption, Encryption algorithm, Confidentiality

I. INTRODUCTION

Cloud computing has been envisioned as the next generation of distributed/utility computing. It is defined as a model for enabling suitable, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications) that can be provisioned and produced with minimal management effort or service provider interaction. The National Institute of Standards and Technology (NIST) define cloud computing by five essential characteristics, three service models, and four deployment models. The important characteristics are on demand self-service, location-independent resource pooling, broad network access, rapid resource elasticity, and measured service. The main three service models are software as a service (SAAS), platform as a service (PAAS), and infrastructure as a service (IAAS). The deployment models include private cloud, public cloud, community cloud, and hybrid cloud. Nowadays, cloud-computing model can offer any conceivable form of services, such as computational resources for high performance computing applications, web services, social networking, and telecommunications services. Apart from that, cloud storage in data centers is very useful for users to store and access their data remotely anywhere anytime without any additional burden. However, the main problem of cloud data storage is security. Therefore, cloud data centers should have some mechanisms able to specify storage correctness and integrity of data stored on cloud.

II. LITERATURE SURVEY

In ZaidKartit, Ali Azougaghe , H.KamalIdrissi , M.ElMarraki , M.Hedabou, M.Belkasmi , A.Kartit [1], proposes a simple, secure, and privacy-preserving architecture for inter-Cloud data sharing based on an or encryption idecryption algorithm which aims to protect the data stored in the cloud from the unauthorized access.

In D.I. George Amalarethinam, H. M. Leena [2], Cloud Computing is a distributed and centralized network of inter connected and inter related systems with one or more IT resources provisioned based on pay-on-demand usage. Even though Cloud consumers or users are more flexible with cloud resources, there exist various issues which bring down the usage of cloud resources. Security issue is the major one among them. Data Security and Privacy, Identity and Access Management, Disaster Recovery/Business Continuity Planning etc., are some of the crisis related to data stored on the cloud. Since the cloud users are more concerned with their data, its security is a major issue which has to be dealt seriously. Securing the users' data can be achieved by the conventional method of Cryptography. 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 respectively 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.

In Akhil K, Praveen Kumar M,Pushpa B.R [3], Cloud computing is the revolution through which individuals can share resources, services and data among the users through the network. Since millions of users uses the same network for data transfer, the data becomes more vulnerable to different security attacks from intruders. Providing security to these data has

become the critical area of concern. The current system for data security concentrates on providing security to the stored data in cloud storage but concerns less on securing the data while it is being transferred. The data becomes prone to intruder attacks while being transferred. Also, in the current existing trend, the third party auditor is given access to data during data transfer. This also increases the access vulnerability of data as the intruder could act as third party and gain access to the data. Considering security as a crucial issue, the system proposed concentrates on providing security to transferring data using encryption technique. The system also takes into consideration the issue concerned with the third party auditor, that in the proposed approach, the auditor is denied access to the user data. Experiments are conducted and have shown that the proposed approach increases the overall security of system by making it difficult for intruders to crack the data being transferred.

In D.I. George Amalarethinam, B. Fathima Mary [4], Data storage security is a highest concern in the cloud storage. Cloud offers huge amount of space to store their user data. This technology has proved itself as a new venture because of its ability for releasing massive computational storage with reducing cost from anywhere to any user at any time. User outsources their data to the cloud for flexible, efficient and seamless services. Once the data is sent to the cloud, the cloud service provider (CSP) alone is responsible for the data. Apart from the benefits, it has lot of security issues on the data stored in the cloud. When a user outsources the data to the cloud, there is possibility to attack the data at rest as well as data in transit. Now the concern is how to secure the data and rely on the services in cloud. In order to protect the data from unauthorized access, data should be in either encrypted format or masked format. Data security is one of the major issues which acts as an obstacle in the adoption of cloud computing. This paper proposes an elegant and novel method to enhance the security of data by associating obfuscation technique along with steganography. Theproposed confidentiality technique that combines the obfuscation and steganography techniques. The main principal of obfuscation is that transforms data into new form and it must conceal the original data while the steganography hides the existence of information. The obfuscated text can be hidden in image by using Least Significant Bit(LSB) substitution method. The experimental results prove that the proposed technique has high embedding capacity and high quality stego images.

In S. Arul Oli, Dr. L. Arockiam [5], Modern technologies witness lots more developments. Cloud Computing (CC) is one of the rapid developments. The demands, the importance and the usage of cloud computing is on the increase every day. As the importance is on the increase, so are the security problems and its threats. The problems in CC make huge impacts on the developments and its popularity. In CC, the data storage has become an indispensable dimension. The data stored could be either numeric or non-numeric. These data need to be protected with confidentiality measures before storing it in the CC. The encryption method comes into an aid for depositing the data into cloud database. The cryptographic techniques are used to enhance the security. This paper proposes a CT to enhance confidentiality of numerical and non-numerical data in cloud through AO_ARO_EncObfus_CT. The technique is used by obfuscation and encryption methods. This paper also suggests the technique to enhance security level. The paper produces minimum time, data size and service while uploading into the cloud storage.

In KajalRani , Raj Kumar Sagar [6], Now days cloud computing become one of the main topic of IT and main point is cloud data storage security. Cloud computing is the fastest growing technology. This technology provides access to many different applications. 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. It provides high quality applications. As we proposed the concept of cloud data storage security strategy capable to overcome the shortcomings of traditional data protection algorithms and improving security using steganography, encryption decryption techniques, compression and splitting technique adoptable to better security for the cloud. We have developed a desktop application through which user can share data. This paper enhanced advance security goal for cloud data storage.

In Vikas K.Soman ,Natarajan V [7], the security of data in the cloud is important as the cloud applications data loss and leakage is very high these days. The data is accessible from anywhere at any time and it is important to make a secure cloud system so that confidentiality and integrity are to be achieved. This paper proposes an enhanced hybrid data security algorithm for the cloud to secure data protection of the cloud.

In R. Swathi, T. Subha [8], Cloud computing is a type of online based computing that gives shared computer dealing out resources& data to the computers. It is dreadfully challenging part to maintain the safety of all required data that are wanted in various applications for the user in cloud. The data stored in the cloud may not be wholly responsible. So, the cloud storage contributors are in charge for monitoring the data which is available and accessible on the cloud, and the physical environment protected and running. There are still some interesting challenges on maintaining the truthfulness of full data that is stored up in the computing environment. The stored data in cloud is so important that the users make ensure either the data is corrupted or lost. This work studies the problem of ensuring the security and integrity of data storage in Cloud Computing. This paper, proposes an approach named enhancing data storage security in cloud using Certificate less public auditing scheme which is used to generate key value. Key Generation Center (KGC) will generate only the partial key so that at any case it will not compromise user's private key. Private & public key is generated based on the partially generated private key by the KGC and to check the cloud data reliability of the user's uploads the data in server and then during the auditing of the reliability of data is checked. Once after checking it then sends the report to the users'. To confirm the data reliability during the auditing process &the server generates the proof and randomly selects the blocks. The TPA then

authenticates the proof against cloud server & the auditing result is sent to the user. A detailed execution analysis exhibited that the proposed approach gives preferred execution over the current works.

In K. Sathesh Kumar, K. Shankar, M. Ilayaraja, M. Rajesh [9], recently, a standout amongst the most vital difficulties is the security of cloud computing. In contrast, the security of access is needed and private information in banks, organizations and so forth is completely crucial. Security is the fundamental objective of any innovation during which unapproved interloper can't get to your record or data in the cloud. In our paper, we have proposed the different encryption strategies are cloud sensitive data security process. On the off chance that the data owner stores the sensitive data to cloud server, the data owner is encrypted their data encryption systems. Here, AES, RSA, Blowfish and ECC encryption techniques are considered. From the security model, the most data secure in blowfish encryption contrasted with various different procedures in view of encryption and decryption time with data.

In Tarana Singh, NidhiSaxena [10], Cloud computing is one of the best ever growing internet based expertise that facilitates users to utilize services by making use of large poll of resources without installation of any software. Adoption of this technology is increasing fast because of many advantages including reduction of cost and IT load. Regardless of the recognition of cloud computing, it faces many difficulties such as security that is one of the major inhibitors in the growth of cloud computing. Data confidentiality is one of the security concerns for this technology. Many methods have been introduced to conquer this issue; encryption is one of them and widely used method to ensure the data confidentiality in cloud environment. In this study, an effort is made to review the encryption techniques used for the data confidentiality. The results of review are classified on the basis of type of approach and the type of validation used to validate the approach.

In Ramalingam Sugumar, K. Raja [11], Cloud computing refers internet based computing which is used to sharing of services. Different users place their data in the cloud. Hence, the fact that users no longer have physical possession of the possibly huge size of outsourced data causes the data integrity protection in cloud computing a very challenging and potentially difficult task, especially for users with constrained computing resources and capabilities. In the reason of, fitness of data and security is a major concern. The security of cloud computing plays a vital role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. The main issue of cloud storage is to secure the data. Many of the security algorithms are available in the cloud computing environment. This proposed algorithm is also to ensure the data key generation very important. In this proposed method ANENC table is used to generate key and perform several versatile operation used to secure the data in cloud computing.

In M. Thangapandiyan, P. M. RubeshAnand and K. Sakthidasan [12], Cloud computation is an emerging technique of providing data backup and managing applications on centralized servers. The cloud services are dependent on Internet which provides the shared resources to the users during the times of demand. The users can be in a state of mobility, but are still capable of retrieving the data from cloud. These data are open to security attacks. Cloud Service Providers (CSP) need to maintain large quantity of data by overcoming the security threats through adoption of suitable, secure schemes. The cloud data are often required by the users of various interests. In order to provide privacy to sensitive data, a Modified Elliptic Curve Cryptography (MECC) algorithm is proposed in this paper. The proposed algorithm generates separate key for all admins and users to access the data. The data is encrypted and decrypted by utilizing the similar MECC algorithm. Whenever the users and other admins want to access the cloud data, they are verified for their identity. After positive verification, the requesters are provided with attributes. The receivers execute the MECC algorithm and generate private key for decrypting the data with these attributes. This ensures high degree of data encapsulation in cloud computation. Performance comparison between the proposed and conventional schemes are carried out and observed that the MECC algorithm is highly secured than other conventional schemes.

In Amar Meryem, Douzi Samira, ElOuahidi Bouabid [13], many customers ranked cloud security as a major challenge that threaten their work and reduces their trust on cloud service's provider. Hence, an important improvement is required to establish the better adaptations of security measures that suit recent technologies and especially distributed architectures. Considering the meaningful recorded data in cloud generated log files, making analysis on them, mines insightful value about hacker's actions. It identifies malicious user behaviors and predicts new suspected events. Not only that, but centralizing log files, avoids insiders from causing damage to system. In this paper, we offered to take away sensitive log files into a single server provider and combining both MapReduce programming and k-means on the same algorithm to cluster observed events into classes having similar features. To label unidentified user behaviors and predict new suspected activities this approach considers cosine distances and deviation metrics.

In HajarZiglari, SaadiahYahya[14], in order to manage IT, cloud computing adoption is a successful technology for the majority of organizations to have a cost effective strategy. However, security is the major issue that decreases the growth of cloud computing. This article proposes different deployment models based on different security concerns. Each model provides additional security related features to the previous models. The final model eases the security concerns and can be used as a reference model for the deployment models.

In A Venkatesh, Marrynal S Eastaff [15], Cloud computing provides on demand services to its clients. Data storage is among one of the prime services provided by cloud computing. Cloud service provider hosts the data of data owner on their server and user can access their data from servers. As data, owners and servers are different personalities, the paradigm of data storage brings up many security challenges. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper, we will discuss the various techniques that are used for secure data storage on cloud.

In Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi [16], Cloud security is an evolving sub-domain of computer and network security. Cloud platform utilizes third-party data centers model. An example of cloud platform as a service (PaaS) is Heroku. It supports several programming languages that are used for web application deployment model. Heroku is based on a managed container system, with combined data services and a powerful ecosystem, for deploying and running modern apps. One important issue in cloud computing is data security, which is handled using cryptography methods. A possible and widely used method to encrypt data is Advanced Encryption Standard (AES). In this paper, we implemented Heroku as a cloud platform, and then we implemented AES for data security in Heroku. The performance evaluation shows that AES cryptography technique can be used for data security. Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.

In Uma B, Sumathi [17], multimedia is the fast growing technology and almost all the mobile users' need multimedia based applications. As mobile device have limited storage and concurrently it cannot process other multimedia (video) application due to small RAM. Therefore we are using cloud for storing our information. But we cannot assure the security of our stored information in the cloud. The maintenance team of cloud environment may provide copyright protection but there is a chance of stealing/hacking our own confidential information by them. Robust reversible watermarking and RSA digital signature can solve this kind of problem. These two techniques were used after the encryption algorithm and are used to protect the data in mobile cloud environment. It offers better security performance, increase the original information quality and confidentiality.

In Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya, [18], outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other unauthorized users and nodes within the cloud. Therefore, high security measures are needed to protect data within the cloud. However, the engaged security strategy must also take into account the optimization of the data retrieval time. In this paper, we proposed Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively methodologies the security and performance issues. In the DROPS method, we divide a single file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is discovered to the attacker. Furthermore, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS approach does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the possibility to locate and compromise all of the nodes storing the fragments of a single file is really low. We also compare and contrast the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

TABLE 1. COMPARISON TABLE OF DIFFERENT PROPOSALS IN CLOUD SECURITY ANALYSIS

S. No	Title	Techniques	Parameter analysis	Mathematical proof	Future work
1.	Applying Encryption algorithm for Data Security in cloud storage	Symmetric encryption – AES Asymmetric encryption – RSA	Key length	The download time is greater than the upload time. This is explained by the addition of key recovery time on server	To focus on Homomorphic encryption
2.	Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud	Enhanced RSA	Key size	Usage of prime numbers instead of random number increase the strength of key and speed of encryption and decryption process	The time spent for encryption and decryption can still be improved by using the concept of Addition chaining.
3.	Enhanced Cloud Data Security Using AES Algorithm	Symmetric encryption – AES	Verification for authenticity	_	To concentrate on other algorithms and implementing two algorithms in single system to verify data security, authentication and verification
4.	Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography	Combines the obfuscation and Steganography techniques.	Speed, security of data, performance (PSNR- Peak Signal to Noise Ratio).	This has higher PSNR values than method, although more hiding capacity compare than the existing technique.	_
5.	Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to	AO_ARO_EncObfus_CT combines both the encryption and obfuscation techniques AO_Enc_CT and ARO_Obfus_CT	Minimum time, data size and service cost	Provides Minimum time, data size and service cost while using AO_ARO_EncObfus_CT	_

	Enhance Security in Public Cloud Storage				
6.	Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique	Steganography, encryption decryption techniques, compression and splitting technique	High quality services, Minimizing time	_	Try to deploy this in other cloud based environment. We can add training module to our system
7.	An Enhanced hybrid Data Security Algorithm for Cloud	A combination of ECDSA, SHA256 and AES is used for sending and receiving data message on the cloud.	Privacy, Confidentiality, Integrity	_	The comparison of different hybrid cryptographic algorithm for data security in cloud should be performed and efficiency analysis of different large file size with these algorithms is to be carried out.
8.	Enhancing data storage security in Cloud using certificate less public Auditing	KGC key and partial private key Generation and public key generation	Key management	Uploading and encrypting performance is analyzed by the KGC	_
9.	Sensitive data security in cloud computing aid of different encryption techniques	Symmetric encryption – AES Asymmetric encryption – RSA Blowfish and Elliptic curve cryptography - This algorithm is used after RSA	Encryption time, Decryption time, Execution time, Memory	Blowfish algorithm consumes less amount of encryption, decryption, execution time and less memory	The portal between the private and public parts of a hybrid cloud is a fascinating point for future research.
10.	A New cloud security and confidentiality model by encryption and data monitoring	1. RSA 2. Data Encryption Standard 3. Simplifies Data Encryption Standard 4. Secure Socket Layer 5. Mixed encryption algorithms. 6. RC5 7. Role Base Encryption 8. Geo encryption Proxy re-encryption and Hierarchical attribute-based encryption	Validation	It compares the eight recent encryption algorithms and to get the fastest and highest security algorithm which is based on cloud infrastructure.	_
11.	Enhanced Data Security methodology for cloud computing environment	Classical encryption techniques by integrating 1.Substitution cipher 2.Transposition cipher.	Accuracy	Out of 50 words 35 words are successfully encrypted and decrypted. Remaining words are produce a single character error	Improve the accuracy of encryption and decryption for all words
12.	Enhanced Cloud Security Implementation using Modified ECC Algorithm	Modified Elliptical Curve Cryptography	Encryption time, Decryption time, Throughput	It provides an faster performance to the existing schemes like DES, AES, RSA and MD5.	
13.	Enhancing Cloud Security using advanced MapReduce k-means on log files	MapReduce programming and k-means algorithm	cosine distances and deviation metrics	_	_
14.	Deployment Models: Enhancing Security in Cloud Computing Environment	_	Various deployment models are used for different issues	_	The future research on this work will be on the development and the corresponding interfaces and design patterns for

					cloud based applications in order to fit the designed deployment models
15.	A Study of Data Storage Security Issues in Cloud Computing	For ensuring confidentiality, Blowfish encryption algorithm is used for providing integrity is using Message Authentication Code(MAC)	Confidentiality, Integrity, Availability	_	Effective auditing mechanisms also can be used for providing data integrity.
16.	Data Security in Cloud Computing Using AES Under HEROKU Cloud	Symmetric encryption – AES	Size of the uploaded file, the network speed	Delay calculation is done by recording the encryption time for files with a size of 3000 kB, 5000 kB, 7000 kB, 10000 kB, and 15000 kB.	_
17.	An Efficient Approach for Data Security in Cloud Environment using Watermarking Technique and RSA Digital Signatures	Asymmetric encryption – RSA Robust reversible watermarking, RSA digital signature	Less effective, losses in recovery of original image, attacks from unauthorized users.	Analysis of PSNR and robustness of image.	To test implement the same algorithm on video and other multimedia contents
18.	DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security	Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS)	Performance	The higher level of security with slight performance overhead was observed	Save the time and resources utilized in downloading, updating, and uploading the file again.

III. CONCLUSION

This paper covers security issues and various techniques have been used to enhancing security as well as security requirements of an existing Cloud system. A generalized view of these issues has been presented here to enhance the importance of understanding the security flaws of the Cloud computing framework and devising suitable counter measures for them. With the development of new computing paradigm, cloud computing becomes the most notable one, which provides convenient, on-demand services from a shared pool of configurable computing resources. Therefore, in this paper, we collectively approach the issue of security and performance as a secure data replication problem. We present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that wisely fragments user files into pieces and replicates them at strategic locations within the cloud. The divisions of a file into fragments are performed based on a given user criteria such that the individual fragment does not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security.

IV. FUTURE WORK

We proposed the DROPS technique, a cloud storage security scheme that deals with the security and performance in terms of retrieval time. The data file was fragmented into small parts and the fragments are dispersed over multiple nodes. The nodes separated by means of T-coloring technique. The fragmentation and dispersal ensured that no significant information was obtained by an adversary in case of a successful attack. No nodes are in the cloud, stored more than a single fragment of the same file. The performance of this methodology was compared with full-scale replication techniques. The results of the models discovered that the concurrent focus on the security and performance resulted in increased security level of data accompanied by a slight performance drop. Presently with the DROPS methodology, a user can download the file, update the contents, and upload it again. This is one of the strategies to develop an automatic update mechanism that can identify and update the required fragments only. The aforementioned future work will save the time and resources utilized in downloading, updating, and uploading the file again. Moreover, the implications of TCP incest over the DROPS methodology need to be studied that is relevant to distributed data storage and access.

REFERENCES

[1] Zaid Kartit, Ali Azougaghe , H. KamalIdrissi , M. ElMarraki , M. Hedabou, M. Belkasmi , A. Kartit, "Applying Encryption Algorithm for Data Security in Cloud Storage," In: Sabir E., Medromi H., Sadik M. (eds) Advances in Ubiquitous Networking. UNet 2015. Lecture Notes in Electrical Engineering, vol 366. Springer, Singapore, 2014.

[2] D.I. George Amalarethinam, H. M. Leena, "Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud", World Congress on Computing and Communication Technologies, 2016.

[3] Akhil K, Praveen Kumar M,Pushpa B.R, "Enhanced Cloud Data Security Using AES Algorithm", International Conference on Intelligent Computing and Control (I2C2), 2017.

[4] D.I.George Amalarethinam, B. Fathima Mary, "Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography", World Congress on Computing and Communication Technologies, 2016.
[5] S. Arul Oli, L. Arockiam, "Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to Enhance Security in Public Cloud Storage", World Congress on Computing and Communication Technologies, 2016.
[6] Kajal Rani , Raj Kumar Sagar, "Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique", 2nd International Conference on Telecommunication and Networks, 2017.
[7] Vikas K.Soman , Natarajan V, "An Enhanced hybrid Data Security Algorithm for Cloud", International Conference on Networks & Advances in Computational Technologies (NetACT), 2017.
[8] R.Swathi, T.Subha, "Enhancing Data Storage Security in Cloud Using Certificateless Public Auditing", 2nd International Conference on Computing and Communications Technologies (ICCCT), 2017.
[9] K.Sathesh Kumar, K.Shankar, M. Ilayaraja, M. Rajesh, "Sensitive Data Security In Cloud Computing Aid Of Different Encryption Techniques", Journal of Advanced Research in Dynamical and Control Systems, vol. 9, pp. 2888-2899, 2017.
[10] Tarana Singh, Nidhi Saxena, "A New Cloud Security and Confidentiality Model by Encryption and Data Monitoring", International Journal of Engineering Science and Computing, vol. 4, pp. 16831-16836, 2018.
[11] Ramalingam Sugumar, K. Raja, "EDSMCCE: Enhanced Data Security Methodology for Cloud Computing Environment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 3, pp. 40-46, 2018.
[12] M. Thangapandiyan, P. M. RubeshAnand and K. Sakthidasan, "Enhanced Cloud Security Implementation using Modified ECC Algorithm" International Conference on Communication and Signal Processing, 2018.
[13] Amar Meryem, Douzi Samira, El OuahidiBouabid, "Enhancing Cloud Security using advanced MapReduce k-means on log files", ICSIM2018, Association for Computing Machinery. ACM, 2018.
[14] HajarZiglari, SaadiahYahya, "Deployment Models: Enhancing Security in Cloud Computing Environment", 22nd Asia-Pacific Conference on Communications (APCC2016), 2016.
[15] A Venkatesh, Marrynal S Eastaff, "A Study of Data Storage Security Issues in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 1, pp. 1741-1745, 2018.
[16] Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi, "Data Security in Cloud Computing Using AES under HEROKU Cloud", 2018.
[17] Uma B, Dr. Sumathi S, "An Efficient Approach for Data Security in Cloud Environment using Watermarking Technique and RSA Digital Signatures", International Research Journal of Engineering and Technology, vol. 4, no. 2, pp. 1817-1821, 2017.
[18] Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security," IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 303 – 315, 2018.