IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116114

Cloud File Security Using Hybrid Cryptography Algorithms

Swapnil R. Shambharkar[1], Ass. Prof. S. K. Purve[2], Ass. Prof. P. T. Tandekar[3]

SSCET Bhadravati, Department of Computer science and Engineering[1,2,3]

Abstract: So many organizations that are moving from their traditional data storage to cloud storage which provides and efficient way to access the data anywhere and anytime. We know that security in cloud computing is the emerging issue in current time. But the main problem of organization is to use cloud computing in the data security. In this paper we have proposing multi level cryptography best security system in cloud computing. We are using new hybrid approach of symmetric and asymmetric key cryptography algorithms. There are two algorithms that we are using are Data Encryption Standards (DES) and RSA Aag implementing here to provide the multilevel of encryption and description at both sender and receiver side which can increase in their security of cloud storage. As this model the security of this model gives you the transparency to the cloud user as well as cloud service provider in order to reduce the security problems. Also this model increases the data security up to a maximum extent and takes less time in processing the text files as comparing to the other existing system.

Keywords: Data Security, Hybrid cryptography, cryptography, Cloud computing, RSA, DES.

• INTRODUCTION

Cloud computing is a flexible and elastic environment for various computing services such as server, storage, networks development platforms and applications which can be delivered on demand with payment based on usage. The benefits of the cloud computing technologies are cost reduction, fast scalability and good reliability that makes it and attractive and better environment for various organisations.

But security in cloud computing is a very highly emerging issue nowadays. So in this paper we have proposing a multilevel cryptography best security system in cloud computing. We are using a new hybrid approach of symmetric and asymmetric key cryptography algorithms. The security of this gives the transparency to the cloud users as well as cloud service provider in order to reduce the security problems.

Cloud computing is the recent trend that occurred in the computing system environment. This technology advancement has led to an increase number of usage in internet and also in cost of software and hardware. Cloud computing can provides a pool of resources and services to the clients as they need. Hence it killed so much popularity as it provides resources via Internet does optimizing users time and cost. These various resources can be accessed by users are networks, server and storage.

The services that have provided by the cloud are webmail, online business applications, various social networking sites and online file storage. User can access any of this services and resources anywhere with just an Internet connection. They are various of technology that can be credited for being such a success in cloud computing are Utility Computing, Service Oriented Computing, virtualization, etc.

Even they are numerous advantages of cloud computing there are still a few road blocks exist to it being accepted widely. So, the data of organisations and users lies together on a platform that can be access by anyone as they provide control to the third party over their data. So, it is at a risk of being exist by someone who is not authorised. So that can leading to the breach in data.

Therefore the main purpose of this research paper is to provide the information security from different types of attackers by symmetric ki cryptography algorithm to Encrypt and Decrypt the clients information at cloud storage and on the client side.

• SERVICES OF CLOUD COMPUTING

Cloud Computing offers basically three types of services. They are as follows and as shown in fig.1.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116114

A. Software as a Service (SaaS): In Software as a Service, the software and its associated data is hosted onto the cloud environment by the Cloud Service Provider (CSP). It is then provided to users in a pay-per-use manner. However, users are not in control over the network, servers, infrastructure, or even the operating systems. This helps in reducing cost for maintenance and support and also as licensing these traditional packages proves to be more expensive than renting cloud service. Its examples include Salesforce CRM and Google Apps among many others.
B. Platform as a Service (PaaS): In Platform as a Service, users are provided with a stage for them so that they can develop, deploy as well as test their applications. Here, the clients manage applications and information whereas the vendors are responsible for networking, virtualization, runtime, storage, middleware, servers, operating systems, and networking. Google App Engine, Windows Azure are some examples of PaaS.
C. Infrastructure as a Service (IaaS): In Infrastructure as a Service, Virtualization is used extensively. Here, various resources like servers, networking as well as storage are issued to the users in a pay as you utilize manner. The resource demand keeps growing or shrinking according to the user's needs, so to meet them Virtualization is needed. The various examples for IaaS include Amazon Web Services (AWS), and Google Compute Engine

• DEPLOYMENT MODEL OF CLOUD MODEL

There are four various types of Deployment models available in the cloud environment. These are presented in fig.2.
A. Public Cloud: As is suggested by the name, in Public Cloud, public can access the services, that is, they can be accessed by anyone and everyone. Clients share same infrastructure. In other words, multiple customers make use of the computing resources that a single service provider provides. Due to being publicly available, it is less secure.
B. Private Cloud: Private cloud is limited, that is, accessible only to a particular organization. Here, the computing resources are available to this organization only and they control it. Also, due to its private nature, it provides better security than that provided by Public cloud
C. Community Cloud: In Community cloud, several organizations that share same concerns share the cloud infrastructure. Here, either a third party vendor or an organization from the community can host the infrastructure. It can be said as a Private Cloud except that it is accessible by a cluster of organizations.
D. Hybrid Cloud: A Hybrid Cloud is a combination of Private and Public Cloud so that the benefits of both the models can be used. Here, the activities that are crucial are accomplished in Private cloud whereas the other noncrucial ones are accomplished in the Public cloud.

• SECURITY ISSUES IN CLOUD COMPUTING

Cloud Computing has many merits such as it improves flexibility, reduces capital cost and improves accessibility. But despite these it is not widely accepted. The sole reason of this being security. When users store their data on cloud, they give access to a third party and lose sole control over their data. The attackers can take advantage of this and tamper with their data. These attackers may be internal (Cloud Service Provider) or external. Since, Cloud Computing has various technologies; it is prone to the security issues of those technologies as well. These technologies include databases, virtualization, resource scheduling, operating systems, concurrency control, networks, transaction management, and memory management. Therefore, data security is a primary concern, so proper enforcements should be done regarding to it. There are various security issues in Cloud Computing. They are as follows:
A. Data Integrity: Data Integrity is among the key concerns in Cloud Computing. The term Data Integrity is a reference to the fact that data should be unchanged by any unauthorized user or in a way that is not authorized. This ensures that the data is not been tampered with. This can be achieved by Digital Signatures.
B. Data Availability: Availability refers to the data being available and can be accessed by the user on demand. When data is stored at remote locations that are maintained by third party users, there is a risk of service providers' system failures. The data will be unavailable if the cloud is unable to provide service.
C. Data Confidentiality: Confidentiality refers to the fact that no one except the authorized user can get access to their data. Encryption is the technique that can be used to ensure this.
D. Data Location: The Cloud providers have their data centers across the globe. Thus, making the users' unaware about the location where the data is stored. This has a disadvantage as their data can be stored in any country. There can be some important information in the data and, it leaving the country could create issues in some countries as it is illegal.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116114

E. Denial of Service: There is a definite number of requests that a server can handle. Once this limit is reached, the server is overloaded, and we observe an error while trying to access the site. The attackers use this technique so that the authorized users are unable to get the services that are assigned to them. An Intrusion Detection System (IDS) is used to defend against this type of attack.
F. Data Breaches: The information which is reserved on Cloud can be some crucial or sensitive information. Some unauthorized user can steal the data and use against the users targeted. This is one of the principal threats in Cloud security as someone can get access to the data that is kept in cloud. The more the data is exposed, the more the threat.
G. Data Loss: Due to some financial problem or natural disasters, the servers can be shut down, leading to the data either being lost or corrupted in cloud. If there is no backup of the data, it might as well be lost forever.
H. Cloud Service Abuse: Here, the hackers can use social media services to disturb the cloud environment by some understanding and extraction of codes. This might lead to the organizations using cloud to face issues.

• CRYPTOGRAPHY

Secure and confidential communication or data transmission is one of the necessities of the social life. Cryptography manages the security of data which may be stored or communicate over the cloud network. Cryptography in cloud uses the encryption methods to secure data, from unauthorized access, which is stored in the cloud. It gives the permission to the users of cloud for acquiring the shared cloud data easily and safely. The shared data that the cloud service provider hosts is secured by encryption technique. Cryptography techniques can secure tactful data without waiting information exchange in cloud. A huge number of security algorithm for cloud computing have been developed using cryptography techniques, which have become very important for the security of data in cloud environment. Cryptography carried out into two different phases encryption and decryption. Encryption as well as decryption both is important aspects of security. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the assistance of a secret key and, in the decryption process, cipher text is an input which is changed over back to plain text with the assistance of same secret key used in encryption procedure. The combinations of same plaintext with different key generate different cipher text hence secret key should keep secret to provide security. There are many different types of schemes available which are used for encryption constitute of area of study known as cryptography. When two parties communicate, secrecy can be provided via symmetric key encryption. The encryption methods, wherein the sender as well as the receiver both is sharing the same key, are known as symmetric key cryptography, whereas in asymmetric key encryption two different keys are used at sender and receiver side.
A. Existing cryptography algorithm for cloud security
In cloud environments the organization usually stored their data and this data can be accessed anywhere any time, but the data security is the main concern for the organizations in the cloud storage model. In order to offer secure data transmission and communication over the heterogeneous and connected network, encryption models plays an important role. Encryption algorithm used the key for the secure data communication. A key is first agreed upon by the communicating parties and kept secret. Now, the key and the encryption algorithms are utilized for encrypting the message previous to sending it from one party to another. This text obtained, known as cipher text, is received by the other party who then decrypts it taking use of the same key and the decryption algorithm. Here, the key is kept as secret while the encryption and decryption algorithms are the known elements. Aswe now know, the key is known to both the sender and the receiver in this cryptography method, but this key distribution is of great importance and proves to be a very difficult task. In this paper symmetric key encryption method is used, where only a single key used for the encryption anddecryption at the sender and receiver side.In the research work only two encryption algorithm is used from the number of symmetric key encryption algorithm as discussed follow
1. Data Encryption Standard (DES) Algorithm
One of the famous symmetric-key block cipher known as the Data Encryption Standard (DES) had been published in 1977 by NIST. The encryption method of DES is very unique, as it received a receive a 64-bit plaintext at sender end and generates a 64 cipher text at receiver ends. In DES, although the key size is 64 bits but only 54 bits key size is used for encryption and decryption. DES is based on the concept of Feistel Cipher implementation and used 16 round of Feistel structure which helps to generates 48-bit unique key form the cipher as per the predefined DES algorithm as discussed in figure 1.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116114

Initially 64 bit permutation is performed on 64 bit block of data, then it is divided into two halves (i.e.32 bit sub-blocks) represented as L0 and R0 that are passed into the Feistel rounds. This process will repeat till 16 round of the encryption method, as the number of twofold is increased the security level is also increased. In the last round (at 16th round) the pre-output is generated by swapping of L15 and R15 bit quantities. Finally, the inverse function of the initial permutation is calculated by concatenating of [R15, L15].

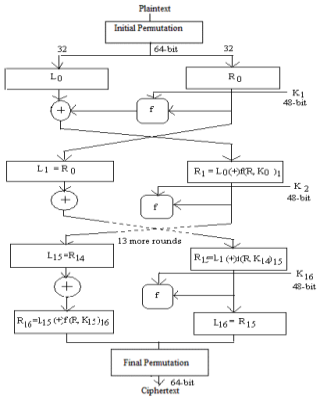
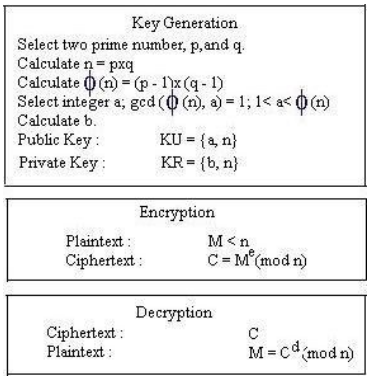


Fig. 1: Encryption with DES

B. RSA Algorithm

RSA is asymmetric algorithm that work on two separate keys considered as public and private key, where public key is shared with all, but private key is kept secret. Rivest, Shamir and Adleman are known as the father of the RSA algorithm. RSA is popularly known for its secure encryption procedure. RSA basically works on positive integer prime numbers that are exponentially used for the encryption and decryption process. The procedure of RSA algorithm is shown in fig. 2 as follow



In this algorithm two exponents variables are used namely e for public and d for private. Here M and C are used as plaintext and cipher text respectively to define the encryption and decryption procedure given as follow

Encryption: C=Me mod n

Decryption: M=Cd mod n.

Where n is a large number, used at key generation time. Shakeeba S. Khan et. al have used the combination of DES and RSA for the secure data storage and communication, but it has some limitation. In this paper a hybrid multilevel encryption and decryption method is proposed to enhance security performance of the existing model.

- **RELATED WORK**

A lot of researches have been made considering security in cloud computing so far. Different authors have suggested different techniques to achieve security considering as the primary concern for the users.

In, Anshika Negi et al. proposed a model where the encryption as well as the decryption method is performed by making use of counter propagation neural (CPN) networks. It is an enhancement on the traditional security system. It discusses about three level authentication mechanisms to improve information security. It does not talk about the

DOI: 10.17148/IJARCCE.2022.116114

performance. The real time monitoring of the system and functioning of the forensic virtual machine is also included in the solution proposed.

Shakeeba S. Khan et al. in proposed a multilevel encryption and decryption algorithm to improve the security with respect to cloud. According to this technique, the attacker or some unauthorized user would have to perform decryption of data at every level, which proves to be a more troublesome task than decrypting it at a single level. The three levels have three different algorithms namely Rivest- Shamir- Adleman (RSA), Data Encryption Standard (DES), and Advanced Encryption Standard (AES) respectively. This aims at shielding the data from an unauthorized access.

Li Chunlin et al. in have addressed the privacy and security issues that exist in cloud computing. They have proposed the use of Ubuntu Enterprise Cloud (UEC) to solve security and privacy issues in cloud computing. This algorithm uses encryption and decryption of data in order to achieve it. UEC ensures the administrators are not getting totally unrestricted access to the client's data in the name of fulfilling their duties. It ensures that the schema of cloud prevents user's data from exposure, thus, maintaining privacy.

H.S. Venter et al. propose a model to reduce the cyber attacks that target the data confidentiality in cloud. To achieve this, they propose client-end encryption and key management. They use chaos and neural cryptography to form a novel cryptography scheme. This scheme is used for improving the strength of the encryption keys by using chaotic random noise as the strength relies on the random nature of input noise rather than the length of the key.

K. Raja et al. propose a symmetric based encryption algorithm for Cloud data security. An alphanumeric encryption table is used to generate keys. These keys are used for primary authentication by users. The usage of this algorithm ensures that data is secured from intruders.

Reshma Suryawanshi et al. in deal with availability, integrity and security of data by introducing two schemes. Public auditing is their first scheme. They use Homomorphic Linear Authenticator as Third Party Authenticator (TPA) in this scheme. Their second scheme, on the other hand, is threshold cryptography. While the first scheme ensures that no knowledge is gained during the auditing process about the important data by TPA; the second scheme ensures that the stored data cannot be misused by any unauthorized user.

Divya Prathana Timothy et al. in proposed a hybrid model that uses Blowfish, RSA, and SHA-2 algorithms. It is a union of both symmetric as well as asymmetric algorithms. Data confidentiality is handled by Blowfish, authentication is dealt with RSA and the integrity of data is handled by SHA-2 algorithm. A high security is provided in this model during data transmission over the internet.

Manju Khari et al. in proposed a Hybrid Encryption Scheme. For user identification and verification, they use a biometric process. The various algorithms used in this paper are Secure Hash Algorithm (SHA), Rivest-Shamir-Adleman (RSA), 3 DES (Data Encryption Standard) algorithms. For uploading the information securely, SHA and RSA algorithms are used whereas 3DES cryptography algorithm is used for data transmission to be done securely. This architecture will create a highly secure environment and also prevent from unauthorized access.

Shilpi Singh et al. in propose a scheme that uses Elliptic Curve Cryptography. Here, the data is encrypted at the client side and can only be decrypted after downloading. Also, at the time of login, the user authenticates themselves via different input parameters. For further security, Elliptic curve cryptosystem (ECC) and Elliptic Curve Diffie-Hellman (ECDH) algorithms are used. They are efficient because key size is less here, and security is much more efficient.

• PROPOSED CRYPTOGRAPHY MODEL

In the current situations the cyber criminals are very active and always wants to hack important data, files and records for the cloud storage, because most of the organizations are using third party cloud services, so cloud security becomes the main concern . In this paper a hybrid multilevel symmetric key and asymmetric key algorithm is developed and implemented where at client side the data encryption is done and then it is uploaded to a web-based cloud storage service. Many service providers, while moving data between their own datacenters do not encrypt it, which may lead to data loss, privacy risks, government intrusions, risk of intellectual property theft issue and spying efforts. Therefore, to deal with such threats, we can encrypt data at client side before we go on to upload it to the cloud storage service. Even though, SSL (Secure Sockets Layer) comes to use for keeping data private as it establishes a link that is encrypted, between a web server and browser while data is in transit , data encryption before being sent adds an extra layer of security to it. Thus, fulfilling the main aim of this algorithm, i.e., to secure data while in transit.

In the proposed model DES and RSA is used for securing the text data during the transmission over the network using encryption and decryption. Whenever any user wants to send the text file, first of all the use has to upload the text file

DOI: 10.17148/IJARCCE.2022.116114

in cloud storage and then in order to increase the security DES and RSA techniques are applied for the decryption on the receiver side when this file is downloaded from the cloud storage. The working of the proposed system is discussed as follow

Sender: Encryption

1. Sender unload the text file on the cloud storage.
2. DES is applied for the first level of encryption and after that RSA is applied for the next level of encryption.
3. Finally the plain text is converted into the Cipher Text, which is stored into the database.

Receiver: Decryption

1. The receiver read the Cipher Text form the database.
2. Now, the RSA algorithm is applied to for the first level of decryption and after that DES is applied for the second level of decryption.
3. Finally the plain text is available for the user.

The proposed model is implemented with two separate cryptography algorithms i.e DES, symmetric and RSA asymmetric in order to increase the security of the cloud. At the sender side DES and RSA encryption are used to encode the uploaded text file. After uploading the test file DES is applied that breaks the data into the blocks of bits and this 64 bits plain text becomes the input of DES that produce 64 bits of cipher text, but the actual key size of DES is 56 bits.

In DES the encryption sixteen Feistel rounds and two permutations (P- boxes) are used to produce the initial and final permutation. The use of 16 iterations in DES means the encryption algorithm is repeated 16 times to generates the cipher text. The security is increased exponentially as the number of iteration increased. Now RSA is applied to generate 2^{nd} level of encryption. After completion of 1^{st} and 2^{nd} level of encryption the cipher text is produced and stored into the database. Once the encryption process is over the multilevel decryption process is started at receiver side by applying inverse DES and RSA algorithms. First inverse RSA is applies to generate 1^{st} level of decryption and then DES is applied to generate 2^{nd} level of decryption, and after successful completion of the decryption process the plain text is ready for display to the users.

CONCLUSION

Nowadays all organizations is following towards cloud environment to store their data as this is emerging trend in data industry, but data security is the main issue in the cloud computing. So in this paper we are composing the multi-level encryption and decryption cryptography algorithm that can encrypt the data from client side after uploading it to the cloud server and decryption process happened at the receivers side which can provide an extra layer of data security. And this paper also shows the various aspect of security issues occurred with the cloud environments at different levels. The DES and RSA encryption and decryption cryptography algorithm are implemented in this paper to increase the security of cloud storage system. In future this model can be implemented using artificial intelligence techniques to enhance the security of cloud services and future works.

REFERENCES

[1] Moulika Bollinadi, Vijay Kumar Damera, “Cloud Computing: Security Issues and Research Challenges” in Journal of Network Communications and Emerging Technologies (JNCET) Volume 7, Issue 11, (2017).

[2] Anshika Negi, Mayank Singh, Sanjeev Kumar, “An Efficient Security Framework Design for Cloud Computing using Artificial Neural Networks” in International Journal of Computer Applications (0975 – 8887) Volume 129 – No.4, (2015).

[3] A Venkatesh, Marrynal S Eastaff, “A Study of Data Storage Security Issues in Cloud Computing”, in International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3-No 1, (2018).

[4] Y Z An, Z F Zaaba & N F Samsudin, “Reviews on Security Issues and Challenges in Cloud Computing”, International Engineering Research and Innovation Symposium (IRIS), Conf. Series: Materials Science and Engineering 160 (2016).

[5] J. Yang and Z. Chen, "Cloud Computing Research and Security Issues," 2010 International Conference on Computational Intelligence and Software Engineering, Wuhan, 2010, pp. 1-3.doi: 10.1109/CISE.2010.5677076.

[6] Deepanshi Nanda, Sonia Sharma, “Security in Cloud Computing using Cryptographic Techniques”, International Journal of Computer Science and Technology Vol. 8, Issue 2, (2017).

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116114

[7] Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan, "Cloud Computing: Study of Security Issues and Research Challenges" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, ISSN: 2278 – 1323 (2018).
[8] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing" in ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering Tome VII [2014] Fascicule 4 ISSN: 2067 – 3809.
[9] N.N Mosola, M.T Dlamini, J.M Blackledge, J.H.P Eloff, H.S Venter, "Chaos-based Encryption Keys and Neural Key-store for Cloud hosted Data Confidentiality", in Southern Africa Telecommunication Networks and Applications Conference (SATNAC) (2017)
[10] Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", in International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, (2015)
[11] AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", in International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352
[12] Dr. Ramalingam Sugumar, K. Raja, "EDSMCCE: Enhanced Data Security Methodology for Cloud Computing Environment" in International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3 | Issue 3 | ISSN: 2456-3307(2018).
[13] Reshma Suryawanshi, Santosh Shelke, "Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme", in International Conference on Computing Communication Control and Automation (ICCUBEA),(2016).
[14] Timothy, Divya Prathana and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS) (2017): 1-5.
[15] Khari, Manju, Manoj Kumar and Vaishali. "Secure data transference architecture for cloud computing using cryptography algorithms." 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (2016): 2141-2146.
[16] S. Singh and V. Kumar, "Secured user's authentication and private data storage- access scheme in cloud computing using Elliptic curve cryptography," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, (2015), pp. 791-795.
[17] K. Brindha and N. Jeyanthi, "Securing cloud data using visual cryptography," International Confernce on Innovation Information in Computing Technologies, Chennai, (2015), pp. 1-5.
[18] Prerna and Parul Agarwal, "Cryptography Based Security for Cloud Computing System", International Journal of Advanced Research in Computer Science, Volume 8, No. 5, (2017).
[19] Dharitri Talukdar, "Study on symmetric key encryption: An Overview", International Journal of Applied Research. (2015); 1(10): 543-546.
[20] Gary C. Kessler, "an Overview of Cryptography", Embry-Riddle Aeronautical University - Daytona Beach, (2016)
[21] David G. Rosado, Eduardo Fernandez-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, (2013).
[22] Dr. Tomislav Nad,"Advances and Trends in Cryptography", SIGS Technology Summit, (2015).
[23] A Survey on Packrat Parser by Prof. S. K. Purve