ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey of Data Security Issues, Data Encryption Techniques and Data Protection in the Cloud Environment

R. Anitha, V. Suganya

Asst. Professor, Department of Computer Science and Engineering, Valliammai Engineering College, Tamil Nadu, India

M.E Student, Department of Computer Science and Engineering, Valliammai Engineering College, Tamil Nadu, India

ABSTRACT: Cloud computing is a developing computing model in which resources of the computing infrastructures are produced as services on the internet. It permits business and consumers to use the application without installation and access their personal files on any computer anywhere with internet access. Data security and privacy are the main issues in cloud computing. It becomes a severe problem being data is stored individually over the two major aspects of user's concern in cloud information technology. In this paper, we discuss about the various data security issues and data encryption techniques. It is also summarized about which algorithm is suited for the cloud environment for secret sharing of data. It will be useful to enhance the security of data storage in a cloud.

KEYWORDS**:** Data Security, security issues, data privacy, encryption, cryptographic keys.

I. INTRODUCTION

Cloud computing may be a model for convenience and on-demand network access to a shared pool of configurable computing resources which will be quickly provisioned and free with minimal management efforts. In easy words, Cloud Computing is that the combination of a technology, platform that has hosting and storage service on the web. The Main goal of the cloud computing is to supply scalable and cheap on-demand computing infrastructures with smart quality of service levels. Several corporations developing and offering cloud computing products and services however havenot properly thought of the implications of the process, storing and accessing information in a very shared and virtualized environment.

Cloud computing as a unique technology for process and transferring information electronically is today employed in nearly each computer system. It runs on a network infrastructure that's opened for various kinds of attacks. DDoS (Distributed Denial of Service) is one amongst the foremost famed attacks that are used. Syn cookies moreover as limitation of the users that are connected with the cloud technology to the server can be used as measures for stopping Distributed Denial of Service. Another variety of attacks on the cloud computing technology are man within the middle attack. Secure Socket Layer (SSL) is a security technique to beat this sort of attack. So, if this security technique isn't organized properly, authentication of the shopper and also the server won't perform because it should protect the users of the cloud technology from the man within the middle. So, security challenges of information protection once exploitation cloud computing should be appropriately solved and decreased.We have a tendency to oncewe after us utilize cloud computing we run our package on onerous disks and CPUs that don't seem to be before people. That's why users are having additional doubts regarding the safety problems after they are exploitation this technology. So, loads of various kinds of attacks might happen within the cloud technology. Besides the higher than mentioned, most famed attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are loads of security techniques for information protection that are accepted from the cloud computing suppliers, and that they all give authentication, confidentiality, access management and authorization.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

II. RELATED WORK

A review of information security problems in cloud surroundings given by SahilZatakiya et al. [1] Authors same that cloud computing is a novel pattern of computing wherever resources are provided on demand via web usage. Here, the author mentioned and analyzed security and privacy problems connected with the cloud and its information storage. They additionally discuss regarding numerous attacks over cloud computing. Here, the authors were talking regarding completely different security issues and attacks on cloud computing setting. During this paper they determine some challenges like security problems, knowledge challenges and additionally offer solutions concerning those problems. They additionally include some attacks with their properties. The huge challenge is that to create knowledge, terribly secure and consumed performance price is a smaller amount than others [1]. Jun Hu et al. [2] Addresses knowledge security access management model of sacred knowledge accessing supported MAC access management, that origins from the govt cloud platform construction. This model includes necessary technical methods to confirm the safety of knowledge accessing. They additionally study regarding the connection of risk issue and expected solutions. Here, the authors were talking regarding knowledge access security model and offers knowledge access method when the 3-stage management technology. So, the main action is high reliability will give a reference for the govt of cloud construction [2]. An ascendible and economical, user authentication, theme for cloud computing environments presented by FarazFatemi M. et al [3]. Here, they projected an economical and scalable user authentication, theme for cloud computing. The outline of this paper is that, planning this user authentication and access management model can enhance the dependableness and rate of trust in the cloud. During this there are 2 separate servers that stores authentication and cryptography resources from the actual servers to decrease the dependency of user authentication and cryptography method from the main server. This model provides reliability too [3]. N Hemalatha et al. [4] Addresses a comparative analysis of cryptographic techniques and knowledge security problems with cloud computing. During this paper they discuss a perspective of cloud computing technologies essential characteristics, classification, delivery models and numerous encryption mechanisms. When finding out and comparative study created on many

Encryption techniques are used for maintaining security and confidentiality over a cloud [4]. Authors additionally classified cloud computing in numerous components. Here, they additionally point out information, integrity, information security, information storage, data backup and recovery, dataconfidentiality and every one. The most challenge is to produce security and privacy to protect information in the cloud. Here, they analyze the importance of information privacy and security. They compare numerous cryptography techniques utilized in a cloud environment [4].

III. VARIOUS TYPES OF DATA SECURITY ISSUES IN THE CLOUD

Whenever a discussion regarding cloud security has taken place there will be great to do for it. The cloud service supplier for cloud makes positive that the client doesn't face any problem similar to loss information of knowledge or data theft. There's additionally an opportunity wherever a malicious user can penetrate the cloud by impersonating a legitimate user, thereby infecting the complete cloud. There are four types of problems raise whereas discussing security of a cloud. In Fig.1.Cloud Data Security Issues, it shows the types of security issues in the cloud environment.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

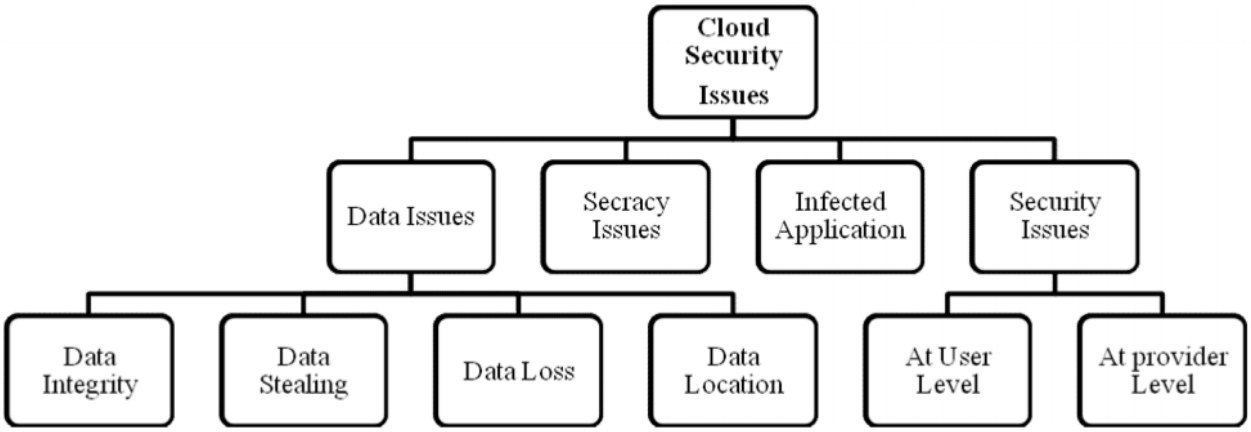

Fig.1. Cloud Data Security Issues

Data Issues: sensitive information in a cloud computing surroundings emerges as major problems with regard to security in a very cloud primarily based system. Firstly, whenever a information is on a cloud, anyone from anyplace, anytime will access information from the cloud since information could also be common, private and sensitive information in a very cloud. Therefore, at a similar time, several cloud computing service shopper and supplier accesses and modify information. Therefore, there's a requirement of some knowledge, integrity, technique in cloud computing. Secondly, information stealing could be a serious issue in a cloud computing environment. Several cloud service suppliers don\'t give their own server instead they acquire server from alternative service suppliers because of it is price emotive and versatile for operation and cloud supplier. Therefore, there's a way chance of information is taken from the external server. Thirdly, knowledge loss could be a common downside in cloud computing. If the cloud computing service provider back up his services due some money or legal downside, then there will be a loss of knowledge for the user. Moreover, information is lost or injured or corrupted due to miss happening, natural disaster, and fire. Because of higher than condition, information might not be accesses able to users. Fourthly, information location is the problems what needs focus in a cloud computing environment. Physical location of information storage is incredibly necessary and crucial.It ought to be clear to user and client.

Secrecy Issues: The cloud computing service supplier should confirm that the client personal data is well secured from different suppliers, client and user. As most of the server area unit external, the cloud service supplier should confirm who is accessing the info and who is maintaining the server so it alter the supplier to safeguard the customer's personal data. Infected Application: cloud computing service supplier should have the entire access to the server with all rights for the aim of observation and maintenance of the server. So this will stop any malicious user from uploading any infected application into the cloud that will severely have an effect on the client and cloud computing service. Security issues: cloud computing security should be done at 2 levels. One is on supplier level and another is on user level. The cloud computing service supplier should confirm that the server is well secured from all the external threats it should come across. Although the cloud computing service supplier has provided an honest security layer for the client and user, the user ought to confirm that there should not be any loss of information or stealing or tampering of information for different users who are mistreated constant cloud thanks to its action. A cloud is good only if there's smart an honest, decent security provided by the service supplier to the user.

The other kinds of problems are Denial of Service (DoS) attacks: As the cloud is shared by several users, DoS attacks way more damaging. Aspect Channel attacks: By inserting a malicious virtual machine to a target cloud server, an attacker will launch an aspect channels attack. Authentication attacks: There are many alternative ways that of the attacker, and strategies used are a frequent target of attackers. Man-in-the-middle Cryptologic attacks: it\'s dispensed once an attacker places himself between 2users. Inside-job: Here person, worker or staffs who have the information about thesystem will attack the cloud system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

IV. VARIOUS TYPES OF DATA ENCRYPTION TECHNIQUES FOR DATA STORAGE SECURITY IN CLOUD ENVIRONMENT

The encryption algorithm is most typically used technique to protect information among cloud surroundings. Concerning a consumer will be categorized as public information and personal data. The general public knowledge is sharable among trusted providers that give are open surroundings for collaboration. Nonpublic information is the client's confidential information that has to be transferred in encrypted type for security and privacy.

To secure the info that is uploaded by users into the cloud, it's to be encrypted. Data in cloud data centers isEncrypted by the user's mistreatment several cryptography techniques.

Cryptography is that the art and science of achieving security by cryptography messages to form them non-readable". The plain text message is in easy English language that may be understood by any. The message is codified mistreatment cryptography techniques known as the cipher text message.We have 3 varieties of techniques1) Symmetric Key Cryptography 2) Asymmetric Key cryptography 3) Hash function Cryptography.

Symmetric Key Cryptography: Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. In Fig.2.Symmetric Key Cryptography, below diagram explain about the symmetric key cryptographic methods to encrypt and decrypt process.

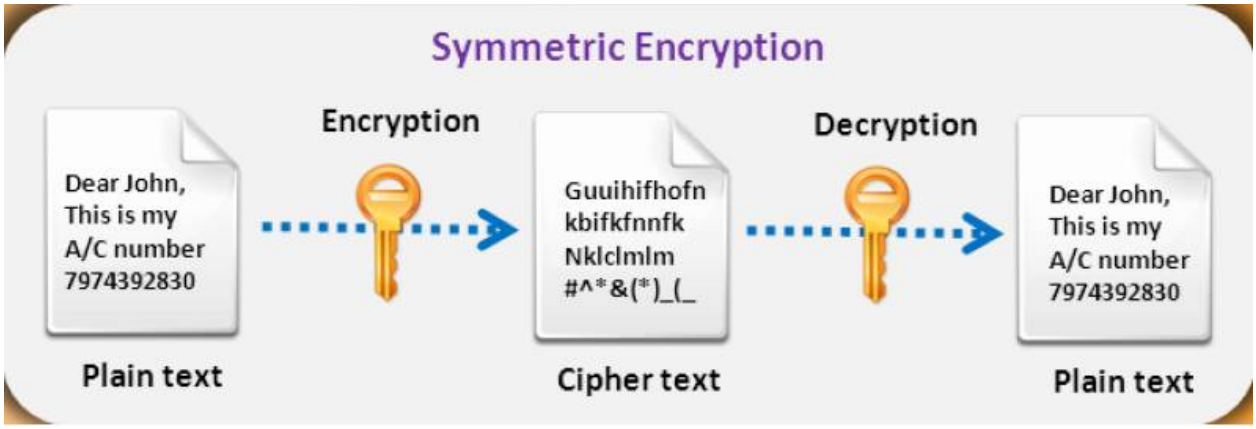

Fig.2. Symmetric Encryption

Asymmetric Cryptography: The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys-a key pair. A public key is made freely available to anyone who might want to send you a message. A second, the private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. In Fig.3.Asymmetric Key Cryptographic, below diagram explain about the asymmetric encryption process in the cloud environment.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

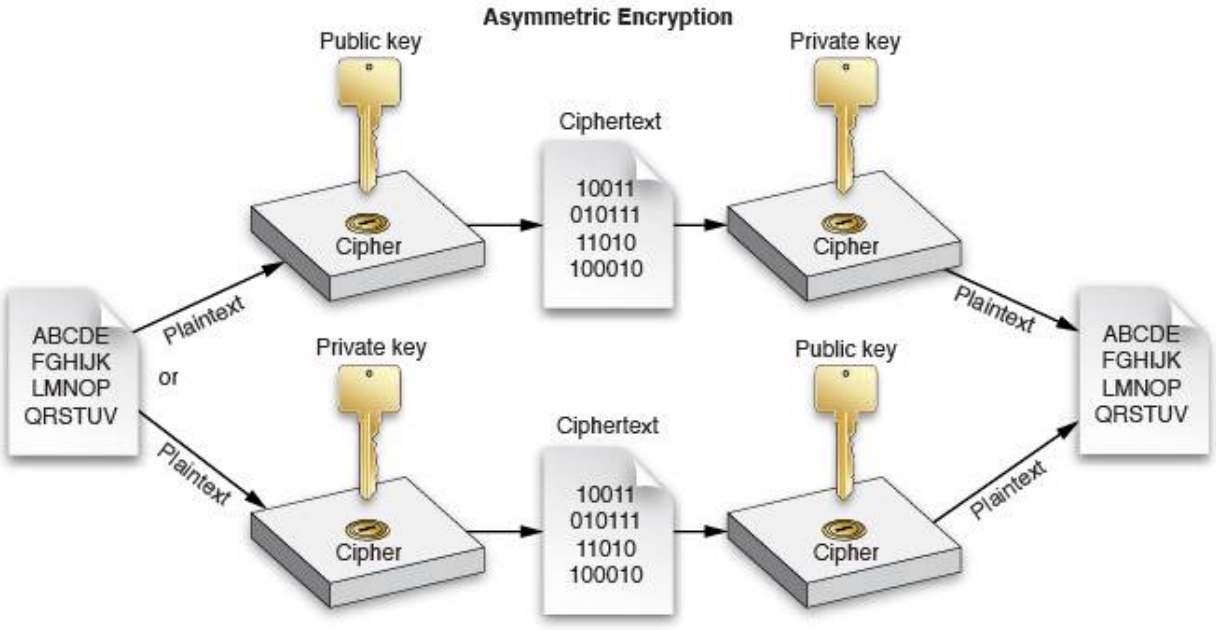

Fig.3. Asymmetric Encryption

Hash Function Cryptography: The hash function cryptography (One way cryptography) offers a way of creating a fixed size block of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digests or one-way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages [11]. The most used hash function cryptography techniques are: SHA1, MD5.

Some encryption techniques for data security in cloud

Encryption is converting clear text into ciphertext. It ensures the confidentiality, and protects the information from unauthorized people during transit over an unreliable network, or during storing in untrusted storage. In this section, we give a brief overview over some cryptographic methods.

AES

AES is the symmetric key block cipher algorithm with which we can provide data security of cloud computing. This block cipher uses 128 bit block size and key length can be 128, 192, and 256. It means for 128 bit key length AES performs 10 rounds, for 192 bit key it performs 12 rounds and for 256 bit key it will performs 14 rounds. All of these rounds perform some steps. Key expansion, Pre round, rounds and last final round.

Advantages of AES:

AES performs well in both software and hardware platform under a wide range of environments. It provides Inherent facilities with which processor, resulting in very good software Performance. AES has speedy key setup time and good key ability. Less memory for implementation. Good potential for benefiting from instruction level parallelism. No serious weak keys in AES

Attribute-Based Encryption

Another set of cryptographic techniques is attributing-based encryption (ABE). It can be a suitable approach when we need each user to be able to decrypt only his authorized data. Therefore, the decryption will only work if there is a match between the attributes associated with the decryption key and the policy used to encrypt a message. This flexibility makes it an attractive choice for cloud computing. It has developed into two branches, which are: key-policy

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). KP-ABE.KP-ABE: combines the access policy with keys corresponding to attributes. CP-ABE: allows the specification of a decryption policy to be associated with a cipher text.

Proxy Re-Encryption

In this scheme a semi-trusted proxy is used to replace a ciphertext that can be decrypted by user A into another cipher text that can be decrypted by user B, without recognizing the original information and user secret keys. Therefore, this approach enables the data owner delegates a third party to perform some computational intensive tasks, such as, re-encryption while leaking little part of the information to them.

Key Store

It is important to manage the encryption keys and store them in a trusted environment to provide a secure storage approach, and prevent an attacker from getting the keys to decrypt the data. Keys are stored on a keystore that can be on one of the following: Portable device: owned by an authorized user within the trusted environment. Specialized server: placed in somewhere, in a trusted environment.

V. PROPOSED METHODS FOR SECURITY OF THE DATA USING BOTH SYMMETRIC AND ASYMMETRIC ENCRYPTION

In this proposed method, we use a combination of symmetric and Asymmetric algorithm for security of data in the cloud. In the proposed system, both Symmetric and asymmetric algorithms are used.The four algorithms are used in this method with a combination of symmetric and asymmetric..A) Elgamal algorithm B) Diffie-Hellman C) Shamir's (k, n) threshold scheme and D) RSA algorithm.

Elgamal algorithm

In this proposed method, elgamal algorithm is used for attribute based encryption. Using this algorithm, attribute keys are generated. El_Gamal is a public-key cryptosystem technique. Elgamal algorithm is used for encrypting and decrypting the file in the cloud environment by the users. In cryptography, the ElGamal encryption system is an asymmetric key e n cryptionalgorithm. In this method, using attributes generate a secret key. That secret key is used for policy file encryption for the security purpose.

DiffeHellman

In this proposed method, this algorithm is used for authentication process between user and key management. It is a method for creating a shared secret numeric key over an open channel with potential eavesdroppers. The two protagonists don't have any (real) control over what the actual number their secret key is. (The key will then be used in a symmetric key algorithm such as DES and AES—see next week's lectures).

Let G = (Z/pZ) ∗be the multiplicative elements mod p. It is a cyclic group of order p − 1. Since it is cyclic, it has a generator g, which means (Z/pZ) ∗= {g, g2,g3…. gp−1}. Using this algorithm generates a secret key between the user and key management. That secret key is used for encrypting the file during upload process.

Shamir's threshold technique

Shamir's (k,n) secret sharing algorithm In this proposed method, this algorithm used for key splitting of a secret key and stored in multiple key managers and reconstruct the keys for security purposes. Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Mathematical definition:

The goal is to divide secret S (e.g., a safe combination) Into pieces of data S1,….,Sn in such a way that:

1. Knowledge of any K or more Si pieces makes S easily computable.
2. Knowledge of any K-1 or fewer pieces

Leaves S completely undetermined (in the sense that all its possible values are equally likely).This scheme is called (K,n) threshold scheme. If k=n then all participants are required to reconstruct the secret. In this method, the secret key is split and send to the multiple key managers. The multiple key managers generate a public key and private key using split keys and then public key only send to user for decrypting purpose when user want download the file.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

RSA

The RSA algorithm is widely used for public key algorithm. RSA is a block cipher in which every message map to an integer.RSA algorithm involves three steps: a) key generation b) encryption c) Decryption.

Steps:

Choose two distinct prime numbers a and b for security purposes, the integers a and b should be chosen at random and should be of similar bit length. Compute n=a*b. Compute Euler's totient function, (n) = (a-1)*(b-1).choose an integer e, such that 1<e<(n) and greatest common divisor of e, (n) is 1. Now e is released as public key exponent. Now determine d. d is multiplicate inverse of e mod (n). D is kept as private key component and public key consists of modulus n and the public exponent e.

These combinations of algorithm are used for secure the data in the cloud compare to other separate encryption algorithm in the cloud data. The proposed method is used in the following model in the system. In this method propose a data security scheme that uses keymanager servers for the management of cryptographic keys. Shamir's(k,n) threshold scheme is used for the management of keys that uses k shares out of n to rebuild the key. Therefore, cryptographic keys must be stored in a powerful manner and a single point of failure should not affect the availability of data. To avoid man in the middle attack user can access their key and data is ensured through a policy file that states policies under which access is granted to the keys.In.Fig.4.Architecture of proposed system, below diagram explain about the proposed system of data security in cloud environment. The data security in the cloud environment makes use of both symmetric and asymmetric keys that are secured by using asymmetric keys. Asymmetric key pairs are generated by the third party key managers. Out of the key pair, only the public key is transmitted to the client. For the secure transmission of keys, a secret key is established between client and key managers through stationto station protocol.

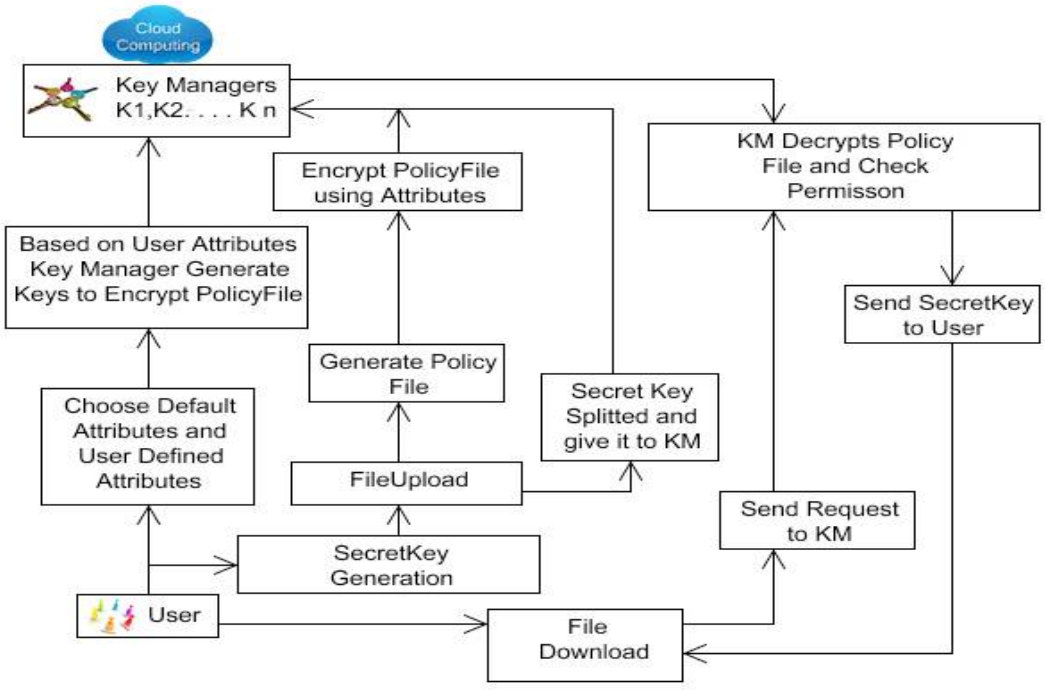

Fig.4. Architecture of Proposed System

Generally, the user has to register to become a member in the cloud. In the proposed model, once user registered to cloud and then the user has to choose some attributes to set a policy. There are two types of attributes in this method. One is default attributes and another one is user defined attributes. In Default attributes, the user has to choose some attributes like name, email, address, etc. In User defined attributes, the user has to give any one of the interested name

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

or place for encrypting their policy file securely. Policy file is created when the user file uploading. After policy setting, Key manager generate a key to encrypt the policy file. The policy file contains username, filename which is uploaded by the user. In this method, attribute based encryption is performed by Elgamal Algorithm After registration, the user has to login into the cloud using username and passwords. Using authentication process, key manager creates a secret key for file encryption. The secret key created by the key manager using Diffie Hellman. After that, a user using keys encrypt the file and upload into the cloud. Key managers split the secret key and send to the splitting key to multiple key managers. Key managers create a public and private key for that own key. The key splitting process is done by using Shamir algorithm. All key managers send the public key to the users for the purpose of decrypt file when download. Simultaneously during the file upload process, policy file is generated. In the policy file contain username, filename which is uploaded by the user. This policy file is also encrypted using a secret key and stored in the cloud. The secret key is generated by the user defined attributes. If users need to download the files, the user first need to login into the cloud account and select download. The user chooses the filename to be downloaded and attributes are given as input. After that, send a request to key manager will check the attributes following the authentication process. Key Manager will provide the decrypted i-th share key. After, that user will download their files securely in the cloud.

VI. CONCLUSION

Cloud computing is a promising and developing way for data transmission and data storage. Cloud computing has many advantages, but still many actual problems that need to be solved. The main issues are data security and privacy. In this paper we analyzed various security issues in cloud computing based upon the previous works which is described in related work and also presents various algorithms for secret sharing of data in the cloud computing. It will be useful to enhance the security of data storage in a cloud. In future we can use the advanced technique methods or algorithms for secure the data in cloud computing.

REFERENCES

1. SahilZatakiya, Pranav Tank, A Review of Data Security Issues in Cloud Environment, International Journal of Computer Applications – IJCA, page – 14-18, 2013, volume- 82.
2. Jun Hu, Lei Chen, Yunhua Wang, Shi-hong Chen, Data Security Access Control Model of Cloud Computing, International Conference on Computer Science and Application - IEEE, 2013, page 29-34.
3. FarazFatemiMoghaddam,ShivaGerayeliMoghaddam,SohrabRouzbeh, SaghebKohpayehAraghi,NimaMoradAlibeigi,ShirinDabbaghiVarnosfaderani, A Scalable and Efficient User Authentication Scheme for Cloud Computing Environment, IEEE – s2014, page 508-513.
4. N. Hemalatha, A. Jenis, A. Cecil Donald, L. Arockiam, A comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing, International Journal of Computer Applications – IJCA, Page – 1-6, 2014, volume – 96.
5. B.Tejaswi, L.V.Reddy, M.Leelavathi, "A Survey on Secure Storage Services in Cloud Computing", Global Journal of Computer Science and Technology Cloud & Distributed Volume 12 Issue, 0975-4172, 2012.
6. YinqianZhang,AriJuels, Michael K. Reiter, "Cross-VM side channels and their use to extract private keys",ACM conference on Computer and communications security,PP. 305-316,2012.
7. BhruguSevak, "Security against Side Channel Attack in Cloud Computing",International Journal of Engineering and Advanced Technology (IJEAT), Vol-2, Issue-2, 2012.
8. Aye Aye Thu, "Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment",International Journal of Computer Applications,Vol. 67– No.4, 2013.
9. VinayakShukla,ShobhitSrivastava, Nidheesh Sharma, "Cloud Computing: Security Issues and Solutions",International Journal of Emerging Trends & Technology in Computer Science,Vol.3, Issue 5, 2014.
10. Mitchell Cochran,Paul D. Witman, "Governance And Service Level Agreement Issues In A Cloud Computing Environment",Journal of Information Technology Management, Vol. XXII, Number 2, 2011.
11. Grispos, G., Glisson, W.B., and Storer, T., "Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization", 21st European Conference on Information Systems, 5-8, 2013.
12. BijayalaxmiPurohit,PawanPrakash Singh, "Data leakage analysis on cloud computing",International Journal of Engineering Research and Applications,Vol. 3, Issue 3, 2013.
13. V. Shobana, M. Shanmugasundaram, "Data Leakage Detection Using Cloud Computing",International Journal of Emerging Technology and Advanced Engineering, Vol.3, Special Issue 1, 2013.
14. Manas M N, Nagalakshmi C K, Shobha G, "Cloud Computing Security Issues And Methods to Overcome",International Journal of Advanced Research in Computer and Communication Engineering,Vol. 3, Issue 4, 2014.
15. Tomoyoshi Takebayashi, Hiroshi Tsuda, TakayukiHasebe, RyusukeMasuoka, "Data Loss Prevention Technologies", FUJITSU Sci. Tech, vol.46, No.1, PP 47-55, 2010.