IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON ENHANCING DATA SECURITY ON CLOUD STORAGE USING SPLIT TECHNIQUE

Rishabh Mudgal*[1] & Mrs. Kirti Bhatia[2]

*[1]M. Tech Scholar, Department of CSE, Sat Kabir Institute of, Technology & Management, Bahadurgarh, Haryana, India

[2]Assistant Professor, Department of CSE, Sat Kabir Institute of, Technology & Management, Bahadurgarh, Haryana, India

DOI: 10.5281/zenodo.1345682

ABSTRACT

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. In this paper, we make a comparative research analysis of the existing research work regarding the data security and privacy protection techniques used in the cloud computing.

Keywords: Data security, Cloud computing, privacy protection

I. INRTODUCTION

Cloud computing is the developing field in the current time. Cloud computing is characterized as the arrangement of assets or administrations offered through the web to the clients on their interest by cloud suppliers. It passes on everything as an administration over the web in light of client interest, for occasion working framework, system equipment, stockpiling, assets, and programming. As every single association is moving its information to the cloud, implies it utilizes the capacity administration gave by the cloud supplier. So there is a need to ensure that information against unapproved access, alteration or disavowal of administrations and so on. To secure the Cloud means secure the medications (estimations) and capacity (databases facilitated by the Cloud supplier). Security objectives of information incorporate three focuses to be specific: Availability Confidentiality, and Integrity. Privacy of information in the cloud is proficient by cryptography. Cryptography, in current days is considered mix of three sorts of calculations. They are

(1) Symmetric-key algorithms
(2) Asymmetric-key algorithms and
(3) Hashing. Integrity of data is ensured by hashing algorithms.

Information cryptography essentially is the scrambling of the substance of the information, for example, content, picture, sound, features to make the information unintelligible, imperceptible or unimportant amid transmission or capacity is termed Encryption. The primary point of cryptography is to deal with information secure from intruders. The inverse procedure of getting back the first information from encoded information is Decryption, which restores the first information. To scramble information at Cloud storage both symmetric-key and Asymmetric key calculations can be utilized. Cloud storage contains a substantial arrangement of databases and for such a vast database uneven key calculation's execution is slower when contrasted with symmetric-key calculations.

II. RELATED WORK

Data security has become a major problem in IT because of the data to be stored securely in servers. From the perspective of data security, Cloud Computing creates new challenges on security threats for many reasons like external data storage, multi-tenancy, dependency on internet, lack of control over data and also internal security. Traditional algorithms will not be having control over the data that is accepted by the cloud [13] [14] [15].

Cloud computing shifts the data, software and databases to the large data centres (server farms) in which repository is used to store, manage and dissemination of the data. T Boneh et al., [16] use digital signature for fine-grained control over user's security privileges. Raghavendra et al., [17] proposes an efficient approach for keyword search to achieve security on outsourced data by involving index generation method along with splitting method for keyword splitting. These keywords are stored using wildcard based techniques that are stored securely with low cost for storage.

In general, traditional symmetric encryption algorithms, such as DES and AES provide relatively lower security and encrypted data are vulnerable to attacks. Danwei et al. [18] propose a strategy to secure data by splitting the data into sections by using data splitting algorithm which assures data reliability. Prakar and Kak [19] splits the stored data and are stored at distinct places on the network and these pieces are backed up in a single server. Sometimes the clients forget the password that are assigned and these leads to brute force attacks. Mazhar Ali et al., [20] also splits the data in the DROPS methodology into number of fragments which are distributed to multiple nodes. These nodes are separated using T-colouring. The fragmentation and distribution ensures that no single node reveals the information to attackers. The performance and security of the DROPS methodology analysed in terms of retrieval time.

Nayak et al., [21] checks the honesty of the service provider by using data reading protocol. After verifying the honesty of the data stored, a system structure has been designed with three data backups for rehabilitation of data. These backups are residing in different places of primary server. This structure uses SHA Hash algorithm for encryption, SFSPL algorithm for splitting files and GZIP algorithm for compressing the data.

Hiremath et al., [22] first presents the network architecture to deploy and evaluating secure data storage issues and then desired properties of public auditing services which are depended on cloud data storage are encouraged systematically and cryptographically. Patel and Dansena [23] have implemented Trusted Platform Module (TPM) to compute the Trusted Computing Group (TCG) [24]. TPM is also used to generate the keys to decrypt the data.

2.1 Data Availability And Data Privacy

As a various security measure, the data privacy and availability in cloud storage signifies to that the data are usable and accessible when authorized users needs them from any security machine at any time in the cloud. In an earlier stage of cloud computing, cloud data availability was more concern because the lack of reliable infrastructure and mature.Different types of data availability and data privacy based cloud security concept was implemented in the cloud storage as follows. Discuss different challenges faced by data encryption and access control mechanisms based on data availability and data privacy, in addition to, recent improvements to meet those difficulties of data availability and data privacy defense in cloud computing. Cloud computing brings the new issue in the creating a reliable and secure data access and storage,it facility over unreliable or insecure service providers. Data storage integrity is one of the challenging tasks in the cloud. Thus, in [25] author proposes a novel approach for overcome this data integrity issue by using remote data integrity checking protocol, which is based on RSA and HLA signature with the support of public verification. This public verification creates the protocol very flexible. Since the user can direct the data prossession to check the TPA.

The computation world has been changed from centralized into distributed system and now it changes back to the virtual centralization which is known as cloud computing. The empire of the computation has been changed to the location of data and process. A client/customer can hold and control the data and the process of his/her computer in one hand. On the other hand, the client or the customer is unaware of where the process has been made and where the data's are store because, the service and the data maintenance were provided by some purveyor. From this we understand the client has no control on it. The internet is used as the communication media for the cloud computing. The purveyor has to provide some assurance in a service level agreement (SLA) about the security of cloud [26]. The Organization uses the cloud computing to examine the security and privacy issues for their business applications. The security of the cloud is still not reliable, so the purveyor has to provide various services like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS).

Each service relies on its own security issues. So the SLA has to be provided based on every single service and explain the security policies which are implemented in their business. This paper helps the organization to know the issues of the cloud services and the security issues that have to be intimate in SLA. Cloud computing empowers ubiquitous, user oriented, on-demand system access to a shared pool of configurable computing resources that can be quickly provisioned and discharged with limited management effort or service provider interaction. In cloud computing, creating a hook is completely surrounded by a combination of warm and cold air, likewise cloud computing gets an analogy which has an exact obstacle with the appropriate services of security and privacy issues. The author identifies the main issues which have a long-term process of the security and privacy issues.

The cloud computing gathers a big attention on infrastructure architecture, software delivery and development models. Cloud computing inherits the model of grid computing, utility computing and autonomic computing and encompasses it into a distributed architecture. The rapid development of the cloud concerns on a complex problems to identify the success of information systems, information security and communication. This paper is presented based on two processes, 1) to identify the unique security requirements based on the justification of cloud security. 2) To eliminate the potential threat by accepting the viable solution. This paper [27] introduces a trusted third party which risks with assuring specific security characteristics inside a cloud environment. The proposed system of cloud computing is cryptography, which particularly deals with SSO and LDAP, to confirm the authentication, integrity and privacy of data and communication.

Cloud computing has developed diversely with the versatile cloud services, so in order to share the data within a friend circle, the cloud computing environment is an efficient platform. But still it is inefficient concerning with security. The features like Key freshness, Key authentication and the Key confidentiality are to be considered when the cloud utilizes the dynamic group key scheme to share the data. The Key Generation Center (KGC) that have the Dynamic Group key protocol distribute the keys to the members of the group and avoid the members who are not in the group. By using this process the above mentioned features are achieved. Because the cloud environment is not efficient in providing privacy, the access control has been a promising task ever. Hence, in this paper [28], a modification in the usual short group signature scheme is done in order to achieve the strongest access control. This proposed scheme provides the strongest data access and avoid the member list verification. Numerous businesses are depending on the cloud computing that has the radical improvement in recent years. This is because of its smart features, namely low cost, flexibility, scalability and fast start-up. The cloud provides many services like rendering hardware and software to observe the security and various issues regarding the security. So it is necessary to use some algorithm to share the private data securely in the cloud [29]. The nodes in the cloud are assigned with an ID number and it is from 1 to N, this is the anonymous ID assignment technique. It improves the data stored in the cloud and becomes difficult for secure sharing. The ID assignment is done using the central authority. The proposed approach is evaluated along with the existing system and it is based on the Newton's identities and Sturm's theorem.

In [30] author suggested a third party auditing mechanism to authenticate the integrity of data. This process may help to access the whole data and this method guarantee the remote data integrity. But there are some issues like some process do not support the dynamic data or public audibility. Thus, this paper discuss all the aspects of current mechanism and also third party contribution which decides both dynamic and audibility data operations. In [31] it proposes some ideas under a Dynamic Multi-Replica Provable Data Possession scheme (DMR-PDP) that avoids the CSP from duplicitous; DMR-PDP also supports efficient dynamic operations like block insertion, modification and deletion on data duplications over cloud servers. Cloud computing technology is one of the information systems which offered the service to the users on the web as rented base. The organization provides some services to scale-up and scale-down for their internal fundamentals [32]. Usually the purveyor makes the arrangement to provide cloud services. There are some major advantages in cloud computing like flexibility, efficiency, scalability, integration and cost reduction. The organization can deploy their application or run their operation through an advanced virtual space provided by the cloud computing technology. The organizations are hesitating to invest in cloud computing for the disregard of its services. This paper is used to review so many security issues and the tasks are discussed.

The cloud computing is known for its success and popularity which represents the new business and computing model. The cloud service provides features on on-demand services such as storage and bandwidth resources. The cloud computing is depending upon many technologies, business and medias. Cloud computing has a conflict in security from a long term and the main obstacles to the extensive use of cloud computing. The author [33] proposes briefly about the security concern which particularly exists on the cloud computing technique. The basic cloud concepts and the cloud security issues have been discussed. The cloud terminology was discussed in the case study of Amazon web services. The discussion of the current process and the future evolution has been made.

Conclusion

Cloud computing is a developing and auspicious way for data storage and data transmission. Security and privacy becomes the most significant issues against the radical growth of cloud computing. The data storage minimization and reduction in processing cost is essential for the any business, because data and information exploration is very significant for making decisions. So the business organization expects a strong trustworthiness between the business owners and the cloud service providers to transfer their data to the cloud. Numerous approaches and techniques have been proposed for the same problem such as data security and protection in the cloud. But these techniques and approaches have to be more efficient and powerful, so that some necessary improvements have to be done with the portion of cloud computing, that the cloud service consumers should accept. In this paper, various approaches and techniques focusing on the data privacy and security on the data storage in the cloud are discussed where the trustworthiness between the consumers and the cloud service providers are made.

2.2Data Access

Data access refers to a user's ability to access or retrieve data that is stored within a database or other repository. Xu et al., [25] developed CeritificateLess Proxy Re- Encryption (CL-PRE), a new proxy-based re-encryption scheme augmented with certificateless public key cryptography. CL-PRE is used for data storage and also to generate secret key and distributed to users for securely sharing the data. Along with CL-PRE, symmetric data encryption is used for encryption purpose by generating proxy re-encryption keys. The data is decrypted using by using users private key. uses MCL-PKE and Security Mediator (SEM) to get the key that is used to get back partial private key information.

Kaitai and Willy [26] proposed a searchable attribute-based re-encryption system that supports primitives like abilities and flexible keyword update service. This scheme uses a sharing policy in which the data owner shares the data to a specified group of users efficiently that matches to the policy. A separate search keyword is maintained and updated after sharing the data. Bala Chandran et al., [27] propose a new model through distributed auditing mechanism to assure the data correction of the data stored. Neha and Ganeshan [28] use Elliptic Curve Cryptography (ECC) for encryption purpose and connection is established using Diffie-Hellman key exchange mechanism in order to achieve data integrity, reduce loss of data and also securely access the data [29].

Mokhtarnameh [1] proposed a key generation technique for certificateless public key cryptography in order to have one public key for one private key. By using CL-PRE, Bilinear Diffie-Hellman problem is solved. Jianghong et al., [2] propose a revocable-storage identity-based encryption (RS-IBE) [3], which introduces the operations of user revocation and updating of ciphertext to provide the forward/backward security. Hou et al., [4] use the traditional ID-based public key (IPK) cryptosystem and traditional IPK to achieve an efficient two party authenticated key agreement protocol based on certificateless public key encryption scheme. It achieves both forward and backward secrecy. Melissa [5] uses multi-authority scheme which identify the attributes by each user. Identify Based Encryption (IBE) is used to focus on the abilities of decryption of ciphertext. Yinxia Sun and Futai Zhang [6] uses Identity-based Cryptography (ID-PKC) which eliminates the need for certificate by deriving public keys for users directly from their human-memorizable information, such as e-mail address and IP address. The private keys are fully generated by a Private Key Generator (PKG) which inevitably introduces the key escrow problem.

Deepa et al. [7] prevents accessing the data from unauthorized users by proposing a homomorphism based token system to verify the erasure-coded data. Zebin et al., [8] discusses the possibility of exploiting cloud computing architectures for parallel and distributed dimensionality reduction and storing of remotely sensed hyper spectral datasets in large data repositories and presents a cloud computing implementation of the PCA algorithm on Spark platform.

Yang [9] proposes a data access control for Multi-authority cloud storage (DAC-MACS) schemes, a secure data CP-ABE method that was proposed with attribute revocation method to attain both forward and backward security [10]. Bottleneck Problem can be controlled by inter-connecting components of cloud via peer-to-peer routing and also identifies single point failure.

Babaoglu et al., [11] designs a p2p cloud system (P2PCS) that makes use of gossip-based protocol to manage a large unreliable resources pool without any central co-ordinator. Li [12] makes use of ERC in p2p storage that greatly improves data reliability and reduce backup server cost. Reed-Solomom (RS) code is much suited for p2p storage cloud. Sanghamitra et al., [13] use the existing goal based threat modelling approach that enables threat modelling for developing designs for secure systems. Countermeasures of P2P cloud has been modelled using threat-SIG. Ranjan et al., [14] uses the cloud peer that generates VMs network to supporting scalable, selfless service and also load balancing.

Azad and Aftab [15] mainly concentrate on newness in the data after updating, trust between third party, CSP and also authorized user. Authorized users do not have the permission to access the stored data but also can be updated. After updating, only the authorized users can access the updated data but not the revoked users. Revoked users cannot see the updated data; they can access the previous data before updation. Trusted Third Party (TTP) is used to determine the dishonest party. Xue and Hong [16] proposes proxy framework that uses proxy signature schemes to securely share the data. Digital envelopes are used to secure the session keys. TGDH scheme is used to update key pair whenever members leave or joined the group. Proxy re-encryption is used to provide forward secrecy and backward secrecy to reduce the computational overheads.

Internet of Things (IoT) is a platform that anyone can transfer data over a network without any interaction. While storing the data, organizations have options to store on cloud. To achieve this, Jayanth [17] uses role based access policies to provide secure data storage in the cloud enforcing cryptographic technique. Zhou et al. Jiang et al., [18] proposes a data storage framework for storing massive data storage of IoT by combining both structured and unstructured data. This framework combines different databases and Hadoop is used to store and manage different types of data collected by sensors and RFID readers.

III. SECURITY ISSUES TO THE CLOUD

The security necessities of a cloud and non-cloud server farm are genuinely similar. The Cloud Security Alliance's starting report contains an alternate kind of scientific classification in light of diverse security areas and procedures that should be followed by and large cloud arrangement. Some protection and security-related issues that are accepted to have long haul essentialness for Cloud computing are:

A. Governance

Administration suggests administration and oversight by the association over methodology, principles and approaches for application advancement and information innovation administration obtaining, likewise on the grounds that the style, usage, testing, utilize, and watching of sent or connected with administrations.

B. Compliance

Agreeability alludes to an affiliation's obligation to work in concurrence with built up laws, particulars and measures. One with the entire premier basic consistence issues confronting an organization is a data area implies capacity of information or data.

C. Malicious Insiders

This danger is surely understood to most associations. 'Vindictive insiders' effect on the association is significant. Malicious insiders are dangerous which has admittance to the information or data about the association being an individual from the association. As cloud shoppers application information is put away on Cloud storage gave by cloud supplier which additionally has the entrance to that information.

D. Account or service Hijacking

This risk happens because of phishing, misrepresentation and programming vulnerabilities. In this sort aggressor can become acquainted with basic regions onto the cloud from where he can take allow and steeling essential data prompting trade off of the accessibility, honesty, furthermore privacy to the administrations.

E. Hypervisor vulnerabilities

The Hypervisor is the principle programming part of Virtualization. There known security vulnerabilities for hypervisors and arrangements are still restricted and frequently exclusive.

F. Insecure APIs

Unknown access, reusable tokens or password, clear-message confirmation or transmission of substance, resolute access controls or dishonourable approvals, constrained checking, and logging capacities and so forth security dangers may jump out at associations if the frail arrangement of interfaces and APIs are utilized.

IV. OBJECTIVE

The Main Objective are:

- To overcome Cloud Computing Security Challenges
- Techniques for Protecting Data in the Cloud
- Strategies for Secure Transition to the Cloud.

4.1 Cloud Computing Security Challenges

Data protection tops the list of cloud concerns today. “Cloud Computing” study, which measured cloud computing trends among technology decision makers.

When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility intosensitive data.

There are complex data security challenges in the cloud:

- ✓ The need to protect confidential business, government, or regulatory data
- ✓ Cloud service models with multiple tenants sharing the same infrastructure
- ✓ Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- ✓ Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- ✓ Auditing, reporting, and compliance concerns
- ✓ Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- ✓ A new type of insider who does not even work for your company, but may have control and visibility into your data

4.2 Techniques For Protecting Data In The Cloud

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks.

The encryption implementation must incorporate a robust key management solution to provide assurance that the keys are sufficiently protected. It’s critical to audit the entire encryption and key management solution. Encryption works in concert with other core data security technologies, gleaning increased security intelligence, to provide a comprehensive multilayered approach to protecting sensitive data—and mitigate risk in or out of the cloud.

Therefore, any data-centric approach must incorporate encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the requisite level of security. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods.

“It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility,” says Tumulak. He emphasizes that an effective cloud security solution should incorporate three key capabilities:

- ✓ Data lockdown
- ✓ Access policies
- ✓ Security intelligence

4.3 Strategies For Secure Transition To The Cloud

The fundamental key to data security is to protect what matters. Solutions that enable companies to confidently transition to the cloud while still leveraging many of their traditional infrastructure and investments offer significant advantages.

Data Security solves the enterprise cloud security conundrum by protecting data inside of the operating environment while establishing security policies and maintaining control through a centralized management interface. One key differentiator is that works with cloud providers and enterprises to protect data regardless of whether it is located in physical, virtual, or cloud environments. This architecture enables enterprises to control access to the data itself, even as the virtual machine migrates to the virtual and cloud world. Organizations can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments.

V. PROPOSED TECHNIQUE

The proposed algorithm is an attempt to present a new approach for complex encrypting and decrypting data based on parallel programming in such a way that the new approach can makeuse of multiple-core processor to achieve higher speed with higher level of security.

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption.

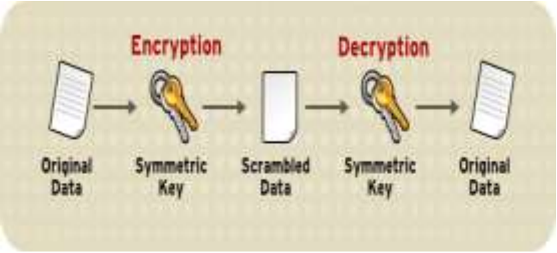
With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a key that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

The sections that follow introduce the use of keys for encryption and decryption.

- Symmetric-Key Encryption
- Public-Key Encryption
- Key Length and Encryption Strength

Symmetric-Key Encryption

With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure.



Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

Symmetric-key encryption plays an important role in the SSL protocol, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, which is described in the next section.

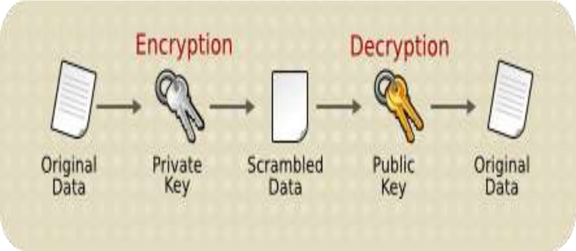
Public-Key Encryption

The most commonly used implementations of public-key encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption.

Public-key encryption (also called asymmetric encryption) involves a pair of keys-a public key and a private key-associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key. Figure 2 shows a simplified view of the way public-key encryption works.



The scheme shown in Figure lets you freely distribute a public key, and only you will be able to read data encrypted using this key. In general, to send encrypted data to someone, you encrypt the data with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol. As it happens, the reverse of the scheme shown in Figure 2 also works: data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it means that anyone with your public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature-an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Firefox can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed. "Digital Signatures" describes how this confirmation process works.

Key Length and Encryption Strength

Breaking an encryption algorithm is basically finding the key to the access the encrypted data in plain text. For symmetric algorithms, breaking the algorithm usually means trying to determine the key used to encrypt the text. For a public key algorithm, breaking the algorithm usually means acquiring the shared secret information between two recipients.

One method of breaking a symmetric algorithm is to simply try every key within the full algorithm until the right key is found. For public key algorithms, since half of the key pair is publicly known, the other half (private key) can be derived using published, though complex, mathematical calculations. Manually finding the key to break an algorithm is called a brute force attack.

Breaking an algorithm introduces the risk of intercepting, or even impersonating and fraudulently verifying, private information.

The key strength of an algorithm is determined by finding the fastest method to break the algorithm and comparing it to a brute force attack.

For symmetric keys, encryption strength is often described in terms of the size or length of the keys used to perform the encryption: in general, longer keys provide stronger encryption. Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher. Roughly speaking, 128-bit RC4 encryption is 3 x 10^{26} times stronger than 40-bit RC4 encryption. (For more information about RC4 and other ciphers used with SSL, see "Introduction to SSL.") An encryption key is considered full strength if the best known attack to break the key is no faster than a brute force attempt to test every key possibility.

Different ciphers may require different key lengths to achieve the same level of encryption strength. The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values.

Because it is relatively trivial to break an RSA key, an RSA public-key encryption cipher must have a very long key, at least 1024 bits, to be considered cryptographically strong. On the other hand, symmetric-key ciphers can achieve approximately the same level of strength with an 80-bit key for most algorithms.

VI. CONCLUSION

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud.

DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithm. DES and AES are mostly used symmetric algorithms.DES is quite simple to implement then AES.

RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data. So we are going to implement Split algorithm so that we can split long file and then after we process the encryption and decryption technique.

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and a symmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of Split algorithm.

REFERENCES

[1] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.
[2] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.
[3] Simarjeet Kaur "Cryptography and Encryption In Cloud Computing", VSRD International Journal of CS & IT Vol. 2 Issue 3, 2012, pp. 242-249.
[4] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.
[5] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.
[6] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Companies, Inc., New York, Special Indian Edition 2007.
[7] Wayne Jansen and Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology, Special Publication 800-144, December 2011, 80 pages
[8] Akhil Behl "Emerging Security Challenges in Cloud Computing ", IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222.
[9] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework"2010 Ninth International Conference on Grid and Cloud Computing.
[10] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" InternationalJournal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp.571-575.
[11] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", InQuality of Service, 2009. 17th International Workshop on, page 19, 2009.

[12] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou “Ensuring Data Storage Security in Cloud Computing.” IEEE2009.

[13] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, “Cloud security issues” In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.

[14] Kashish Goyal, Supriya Kinger” Modified Caesar Cipher for Better Security Enhancement” International Journal ofComputer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[15] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,”Comparison of Symmetric and Asymmetric Cryptography withExisting Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and ManagementStudies, Vol. 11, Issue 03, Oct 2011.

[16] Dan Boneh, Xuhua Ding and Gene Tsudik, “Fine-grained Control of Security Capabilities”, ACM Transactions on Internet Technology (TOIT), vol. 1, no. 4, pp. 60-82. 2004.

[17] Raghavendra S, Girish S, Geeta C M, Rajkumar Buyya, Venugopal K R, S S Iyengar and L M Patnaik, “IGSK: Index Generation on Split Keyword for Search over cloud data”, In the Proceedings of International Conference on Computing and Network Communications (CoCoNet), pp. 374-380, 2015.

[18] Danwei Chen and Yanjun He, “A Study on Secure Data Storage Strategy in Cloud Computing”, Journal of Convergence Information Technology, vol. 5, no. 7, pp. 175-179, September 2010.

[19] Parakh A and Kak S, “Online Data Storage using Implicit Security”, International Journal of Information Sciences, vol. 179, no. 19, pp. 3323-3331, 2009.

[20] Mohamed Ali, Kashif Bilal, Sharifullah Khan, Bharadwaj Veeravalli, Kaicheng Li and Albert Zomaya, “DROPS: Division and Replication of Data in the Cloud for Optimal Performance and Security”, IEEE Transactions on Cloud Computing, ISSN: 2168-7161, 2015.

[21] K Badya Nayak, D Krishna, P Ravindra, “Data Integrity and Dynamic Storage Way in Cloud Computing”, International Journal of Innovative Technologies vol. 3, issue. 2, pp. 0268-0273, ISSN: 2321-8665, June 2015.

[22] Ananda S. Hiremath, Shivaputra S. Panchal, Shriharsha S. Veni, “Providing Security for Data Storage in Cloud through Third Party Auditor”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 7, pp. 379-384, July 2014.

[23] Abhishek Patel, Prabhat Dansena, “TPM as a Middleware for Enterprise Data Security”, International Journal of Computer Science and Mobile Computing, vol. 2, no. 7, pp. 327-332, July 2013.

[24] Matthew Malensek, Sangmi Pallickara, and Shrideep Pallickara, “MINERVA : Proactive Disk Scheduling for Qos in Multi-tier, Multi-tenant Cloud Environments”, IEEE Transactions on Internet Computing, vol. 20, no. 3, pp. 19-27, ISSN: 1089-7801, May-June 2016.

[25] Xu, Lei and Wu, Xiaoxin and Zhang, Xinwen, “CL-PRE: A Certificateless Proxy Re-encryption Scheme for Secure Data Sharing with Public Cloud”, In the Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 87-88, 2012.

[26] Kaitai Liang and Willy Susilo, “Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage”, IEEE Transaction on Informations Forensics and Security, vol. 10, no. 9, pp.1981-1992, September 2015.

[27] R. Bala Chandar, M.S Kavitha, K seenivasan, “A Proficient Model for High end Security in Cloud Computing”, ICTACT Journal on Soft Computing, vol. 4, pp. 694-702. January 2014.

[28] Neha Tirthani, Ganesan R, “Data Security in Cloud Architecutre based on Diffie Hellmam and Elliptic Curve Cryptography, IACR Cryptology e-Print Archive, 2013.

[29] Chen Yang, Furong Wang and Xinmei Wang, “Efficient Mediated Certificates Public-Key Encryption Scheme without Pairings”, In the Proceedings of International Conference on Advanced Information Networking and Applications Workshops, AINAW, vol. 1, pp. 109-112, 2007.

[30] Mokhtarnameh, Razieh and Ho, Sin Ban and Muthuvelu, Nithiapidary, “An Enhanced Certificateless Authenticated Key Agreement Protocol”, In the Proceedings of 13th International Conference on Advanced Communication Technology (ICACT), pp. 802-806, 2011.

[31] Jianghong Wei, Wenfen Liu, Xuexian Hu, “Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption”, Transactions on Cloud Computing, ISSN: 2168-7161, August 2015.

[32] Peng Xu, Tengfei Jiao, Qianhong Wu, Wei Wang, and Hai Jin, “Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email”, IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79, January 2016..

CITE AN ARTICLE

Mudgal, R., & Bhatia, K., Mrs. (2018). A SURVEY ON ENHANCING DATA SECURITY ON CLOUD STORAGE USING SPLIT TECHNIQUE. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 7*(8), 430-439.