ISSN No:-2456-2165

Risks & Solutions for Data Security in Cloud Computing

Mandar Gangurde
MCA
School of Engineering Ajeenky
D. Y. Patil UniversityPune, Maharashtra, India

Abstract:- The safety of one's data when using cloud computing is the topic of this research. It is an investigation into the data stored in the cloud as well as the various issues of data security that are connected to it. In this paper, we will go into the specifics of data protection methods and approaches that are utilized in different parts of the world to provide the highest level of data protection possible by minimizing potential dangers and hazards. The availability of data in the cloud is advantageous for a wide variety of applications, but it also presents hazards because it exposes data to applications that may already contain vulnerabilities in their security protocols. In a similar vein, the utilization of virtualization for cloud computing may put data at risk when a guest operating system is run atop a hypervisor without first determining the dependability of the guest operating system, which may contain a security flaw. In addition to this, the paper will shed light on the various facets of data security that pertain to data both while it is in transit and when it is stored. The research considers all aspects of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Infrastructure as a Service).

Keywords:- *Data Security, Cloud Computing, Data Protection, Privacy, Risks, and threats.*

I. INTRODUCTION

There has been a recent emergence of the term "Cloud Computing," but it is still not commonly used. One of the simplest definitions is "a network solution for offering cheap, dependable, accessible, and simple access to IT resources." The focus of cloud computing is on the underlying services, rather than the applications themselves. Cloud computing's service orientation not only lowers the total cost of ownership and operational expenses but also gives users more control over their systems and better overall performance. Like the transition from traditional computing to a centralized power supply method, cloud computing originates from a single generator at a power steering plant. This means that computer capability can be utilized as a commodity and traded like water or energy.

Internet-based distributed and virtual machine technologiesinspired the concept of cloud computing, which aims to lower the cost of computing by providing consumers with low- priced computer services and storage options. The New York Times rented Amazon's cloud computing capabilities in order to convert over 11 million stories into electronic documents for users to explore, at a total cost of $ 240, which is significantly less than the cost of one of the dozens or perhaps hundreds of traditional alternatives. In addition, the cloud is a highly practical, quick way for a startup to save money on essentials like servers, software, and processing capacity expansion. Unfortunately, cloud computing has not yet achieved the kind of commercial dominance that we had hoped for.

When it comes to adapting cloud storage for data, privacy and data security are important concerns. It is essential for the cloud service to guarantee the confidentiality of the data as well as its own integrity and protection. To achieve this goal, anumber of different service providers are utilizing a variety of policies and mechanisms, each of which is determined by the nature, type, and scale of the data. One of the benefits of usingcloud computing is the ability for several organizations' data to be shared with one another. Nevertheless, this benefit in andof itself constitutes a threat to data. It is imperative that data repositories be protected in order to ward off any potential dangers to the data. When using the cloud to store data, one of the most important questions to ask is whether or not to use a cloud service provided by a third party or to build an internal organizational cloud. Sometimes, the information is too sensitive to be stored in a public cloud. This could be the case with data pertaining to national security or highly confidential information regarding future products, for example. The repercussions of exposing this type of data on a public cloud can be severe because this data might be exceedingly sensitive, and the cloud in question can be public. When this occurs, it is strongly advised that the data be stored using the internal cloud of the organization. Imposing an on-premises data usage policy, this strategy can be helpful in the process of keeping data secure. However, this does not guarantee complete data security and privacy because many firms do not have the necessary expertise to apply all of the necessary layers of protection to sensitive data.

The purpose of this paper is to investigate the methods of data security that are currently in use all over the world to safeguard and protect data stored in the cloud. It examines the potential dangers that could befall data stored in the cloud as well as the solutions that have been implemented by a variety of service providers in order to protect data. growth of computing in the cloud.

II. LITERATURE REVIEW

Several websites have been reviewed in order to acquire an understanding of the fundamentals of cloud computing and the safe and secure storage of data on the cloud. This part presents a review of the relevant literature in order to establish a basis for examining the many facets of data security.

- The authors, Srinivas, Venkata, and Moiz, offer a very helpful introduction to the fundamental ideas of cloud computing. The purpose of this article is to investigate a number of important ideas by examining some instances of apps that may be created with cloud computing and the waysin which these applications can assist developing countries in gaining advantages from new forms of technology.

- On the other side, Chen and Zhao have talked about the customers' worries about shifting their data to the cloud. According to Chen and Zhao, concerns about data security areone of the primary factors that contribute to the reluctance ofmajor businesses to shift their data to the cloud. The authorshave offered an excellent analysis of the data security andprivacy protection challenges associated with cloudcomputing.

In addition to that, they have also talked about some of thepotential remedies that are out there for these problems.

- On the other hand, Hu and A. Klein developed a standard that secures data while it is in transit within a cloud. For the purpose of protecting data while it is being migrated, a standard for encryption has been under discussion. Additional encryption is necessary for strong security, but it requires additional computational resources to implement. The benchmark that was presented in their research offers a compromise that strikes a balance between security and encryption overhead.

- Tjoa, A.M., and Huemer investigate the problem of privacyby giving the end user more control over their data in order to increase confidence.

A number of attacks on cloud computing are discussed here, along with some potential countermeasures to counteract theseattacks.

- In light of this, Abdelkader and Etriby have proposed a datasecurity model for cloud computing that is founded on cloud architecture. In addition to this, they built software in an effortto better enrich the Data Security paradigm for cloud computing.

III. CLOUD COMPUTING AND CLOUD STORAGE

Cloud computing primarily offers two service models: compute and storage. Virtually any service that runs in the cloud needs access to fast, reliable cloud storage to keep up with customer demands. Since data processing is important to modern computer design, it stands to reason that cloud computing companies would also need to offer some sort of cloud storage service.

Multi-tenancy, enormous scalability, elasticity, pay-as-you-go, and self-provisioning of resources are the primary characteristics of cloud computing. There are essentially three distinct types of cloud computing service models. Software as aservice (SaaS) allows users to gain access to software and applications hosted by service providers over the internet, while the other two categories—"infrastructure as a service" (IaaS) and "platform as a service" (PaaS)—provide a virtualized computing environment and online storage, hardware, servers, and networking components. One approach for deploying cloud computing is the "public cloud," which is held by a service provider and from which users can rent or purchase access to the cloud's resources or a privately held or leased cloud infrastructure

The third type of cloud is the "community cloud," which functions similarly to a private cloud but is shared among a smaller group of people.

Cloud infrastructure that combines elements of many deployment types is called a hybrid cloud.

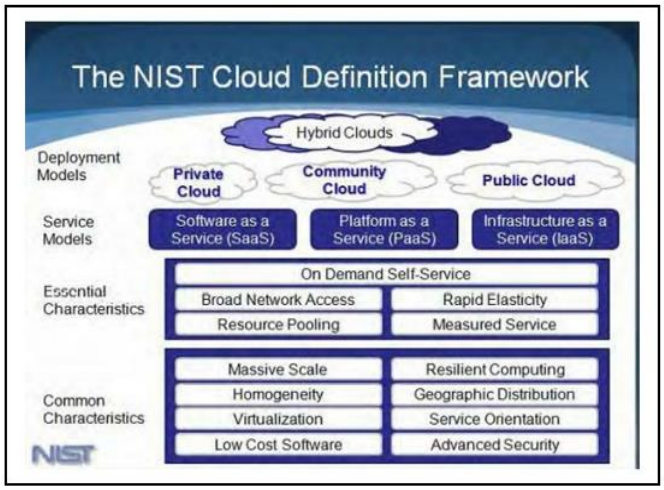

Fig 1:- NIST Cloud Definition Framework

IV. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

As speaking of risks in cloud computing there are 35 risks altogether, classified by ENISA into the following four groups: legal risks, policy and organizational risks, technological risks, and general security risks. The ENISA prioritized these threatsby identifying the top eight. Five of these threats are specifically dedicated to keeping private information secret. Isolation failure, data loss, unsafe data deletion, malevolent insiders, and management interface compromise are allpotential dangers. The Cloud Security Alliance (CSA) also catalogues thirteen distinct threats to cloud services. CSA has identified seven of these threats as being of the highest priority. Account service, traffic hijacking, insecure application programming interfaces, data loss/leakage, and malicious attacks are five of the seven threats that all relate in some way to data confidentiality.

ISSN No:-2456-2165

There are a number of threats and security issues with cloud computing and its data. The virtualization, public cloud storage, and multitenancy that are relevant to cloud computingdata security will be the focus of this research.

➢ *Virtualization*

In virtualization, an image of a fully functional operating system is saved in another operating system so that the real operating system can use all of its resources. To run a guest operating system as a virtual machine in a host operatingsystem, you need something called a hypervisor.

Virtualization is one of the most important parts of cloud computing because it helps deliver the main benefits of cloud computing.

But virtualization in cloud computing brings some risks to data. One risk is that a hypervisor could be hacked. If a hypervisor is weak, it can become a main target. If a hypervisoris broken, the whole system can be broken, which means that the data can also be broken.

Another risk of virtualization is the way resources are givenout and taken back. If VM operation data is written to memoryand isn't cleared before the memory is given to the next VM, the next VM could see the data, which might not be what you want.

Better planning for the use of virtualization is one way to solvethe problems above. Before freeing up resources, they should be used carefully, and data should be checked to make sure it is correct. different service models with varying requirements for protecting sensitive information.

Data at Rest, or information already in the cloud, Data in Transit, or Data in Use, or information leaving the cloud, all pose risks to cloud security. The nature of data procedures, protection measures, and processes determines the data's confidentiality and integrity. This is in three different forms.

➢ *Data at Rest:-*

The term "data at rest" refers to information that is stored in thecloud or any other data that may be accessed via the use of the internet. This covers both active data and data that has been backed up. Because they do not have physical control over the data, businesses that do not keep their data in a private cloud can find it exceedingly difficult, as was said previously, to protect data while it is at rest if they do not have a private cloud. On the other hand, this problem can be overcome by preserving a private cloud that has access that is strictly regulated.

➢ *Storage in Public Cloud*

Another potential security risk associated with cloud computing is the storing of data in a public cloud. Cloud computing typically makes use of centralised storage facilities, which might make them an attractive target for cybercriminals.

If there is even the slightest chance of a security breach in the public cloud, storage resources, which are complex systemsconsisting of a combination of hardware and software implementations, have the potential to expose sensitive data.

It is always advisable to have a private cloud for really sensitive data if one can get one if at all possible. This is so thatsuch hazards can be avoided.

➢ *Data in transit:-*

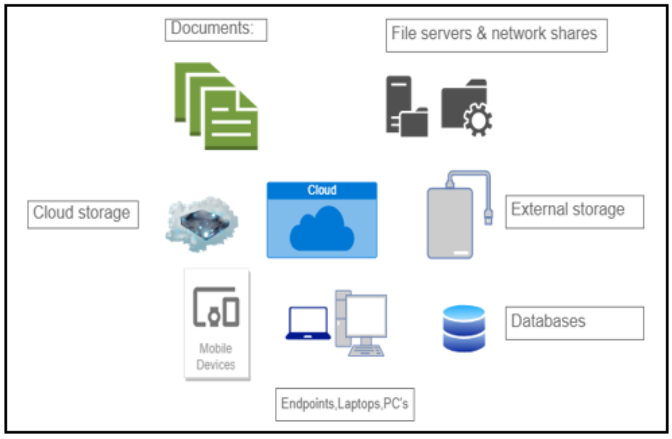

Fig 2:- Data in Rest

➢ *Multienancy*

One of the most significant threats to data in cloud computing is shared access, often known as multitenancy. When numerous users share the same CPU, storage, memory, etc., it poses a risk not just to one but to all of them.

A leak of sensitive information could occur in such a situation. It's important to be cautious with multitenancy attacks because a single vulnerability can give an attacker access to all of the data in the system.

Carefully authenticating people before to granting them access to the data can prevent these kinds of problems.

In order to prevent multitenancy problems in cloud computing,a number of authentication methods are in use.

V. DATA SECURITY IN CLOUD COMPUTING

A side from encryption, data connection is also crucial for cloud computing security. SaaS, PaaS, and IaaS are all The term "data in transit" is commonly used to describe information that is being uploaded or downloaded from a cloud storage service. One can request and use this information fromanother place, as it can be saved in a file or database in the cloud. Data in transit refers to information that has not yet been fully stored in a cloud environment. Passwords and other logininformation are examples of very sensitive data that may require encryption while in transit. Unencrypted data is still data in transit, nevertheless.

➢ *Data in Use:-*

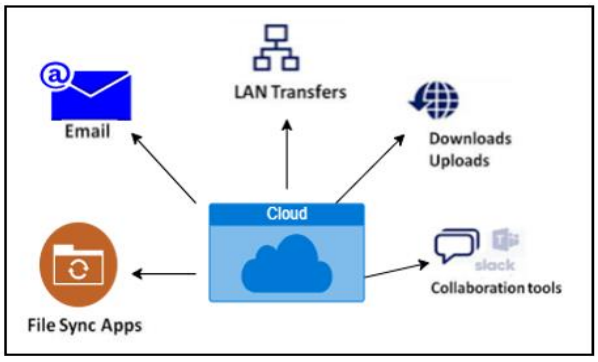

Fig 3:- Data in Transit

into the programme. As a result, consumers are put in a position where they must contemplate the security of their data and applications regardless of who hosts, provides, or mediatesthem.

➢ *Lock-in:-*

Another problem is that there aren't enough data format standards, there aren't enough operating methods, and there aren't enough tools. This makes it hard to move data between services and applications, even between service providers.

So, the customer has to depend on the vendor completely and totally.

➢ *Isolation failure:-*

The sharing of resources that arises as a result of the multi- tenancy feature of cloud computing is in and of itself a Data that is normally being used for processing, such as creation, change, or deletion. Due to the large number of users in the Cloud environment, the chances of mistreatment go up when processing takes place there.

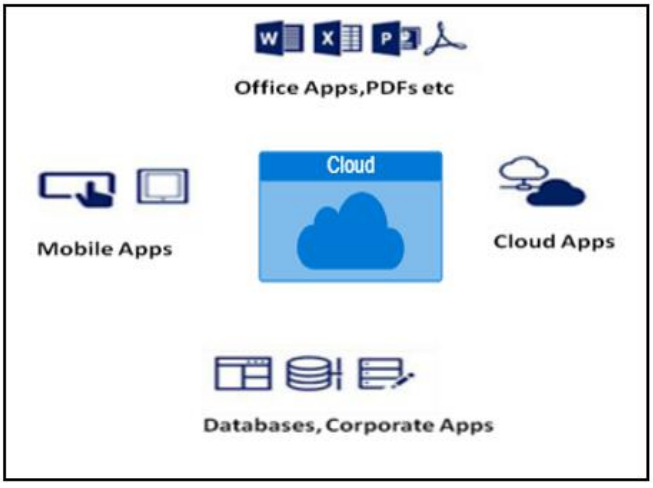

Fig 4 :- Data in Use

VI. MAJOR SECURITY CHALLENGES

Because there are many computers and clients involved, it is not easy to secure and make sure the safety of computers that are linked. This is called "multi-tenancy." The cloud service providers and cloud computing have to deal with a lot of problems, especially when it comes to security. So, it's very important to think about how these challenges are simulated and how security models are put into place to keep clients safe and make cloud computing a safe place to work. The major challenges involved are :

➢ *Lack of appropriate governance:-*

The cloud service provider continues to have full reign over theoperation. When this authority is delegated to the provider, theclient runs the risk of compromising data access and resource utilisation due to a lack of oversight over the authorization parameters. In the absence of a Service Level Agreement between you and your service provider, this security risk posesthe extra risk of leaving you vulnerable. Also, the user is givenconsiderable leeway in how they put the terms of service to use, making it easier for data to be misused. You "accept that Google has no duty or liability for deletion or failure to preserve any material and other communication maintained or sent through use of the service," according to Google's terms of service. Further, Amazon makes it quite clear that they take noaccountability for any harm caused by unauthorised access, usage, corruption, deletion of data, or other forms of intrusion problematic quality. It might be disastrous for companies not tohave adequate space for separate storage. Other concerns surrounding guest hopping attacks and the problems they causeare believed to be a significant obstacle in the utilisation of cloud computing applications and their implementation.

➢ *Malicious attacks from management internally:-*

There is a possibility that consumers' privacy and security could be compromised due to the architecture of cloud computing systems in some cases. This danger presents a significant challenge, despite the fact that it only occasionally materialises. For instance, the administrators and managers of cloud service providers can occasionally pose a security risk to their customers by behaving in a malevolent manner and posing a threat to the clients that use cloud computing services.

➢ *Insecure or incomplete data deletion:-*

When a client asks for some or all of their data to be deleted, itbrings up the question of whether or not it will be possible to delete the right part of their data segment. This makes it harder for clients to sign up for cloud-computing services.

➢ *Data interception:-*

In cloud computing, data is separated and dispersed while in transit, in contrast to traditional computing. This increases risksdue to the insecurity and frailty of computer technology, especially with regards to sniffing and spoofing, third-party attacks, and reply assaults.

➢ *Compromise of management interface:-*

Since cloud services are provided remotely over the Internet and the provider has access to the resources, there is a risk of harmful actions being carried out. As a result, risks, service manipulation, and service provider involvement are allmagnified.

For instance, in some cloud computing use cases, the client may assume ownership of the computers, while in others, the service provider may assume control by instituting strict accesspolicies.

Information leakage during data uploading to the cloud, attacks on privacy and security of user's data, lost or maliciously manipulated encryption keys, and disagreements between service providers and customers on procedure and policies pertaining to the operation of cloud computing applications all pose additional security challenges.

There are also complications that don't directly threaten the security of cloud applications but do interact with or influence cloud computing. Changes in network traffic, network outages, and managerial complications including inefficient resource utilisation, traffic buildup, and lost connections all fall under this category. Social engineering assaults, natural disasters, andtheft of equipment are just a few examples of the additional threats that might impact cloud computing deployments.

VII. PROPOSED SOLUTIONS/APPROACHES TO ENSURE THE DATA SECURITY IN CLOUD

➢ *Encryption:-*

The most popular method for protecting information in the cloud was encryption (used by 45%). To protect cloud information, it is suggested using digital signatures based on the RSA method. Which programme minimises filesize by using a hashing algorithm? The digital signature is generated by encrypting the message digest using the individual's privatekey in software. A digital signature is converted into a messagedigest by software using the recipient's private key and the sender's public key.

Use both the SDES and DES cypher methods for a more secure and robust game (DES). In this method, a 64-bit block of plain text is split in half using a "black box;" the right half contains two bits, while the left half contains six bits. These sixbits are then fed into a "superior function" block, where they are split once again; the first two bits represent the rows, whilethe last four bits represent the columns. Then, the output from the vigenere block is multiplied by this function, which is applied to all eight octets. The output of the black box is 64 bits, which are subsequently subdivided into 4 new octaves. The left half is derived by XOR-ending the right and left halves. At least thrice

The data is encrypted using RSA, and the keys are securely exchanged using Bilinear Diffie-Hellman. The suggested solution adds a message header to each data packet so that clients can securely communicate with the cloud directly, without going through a proxy server. The server generates theuser's public key, private key, and user ID when the userrequests cloud storage. To send data to the cloud, users must first encrypt their data using a private key and append a message header. The SID is looked for in the message header when a user makes a request to a cloud server. If the SID is located, the request is dealt with.

Secure Sockets Layer (SSL) 128-bit encryption, which maybe upgraded to 256 bits, is introduced to guarantee the availability, integrity, and secrecy of cloud data. Access to encrypted cloud data requires a user ID and password. The userinputs data into the cloud, and the cloud service provider encrypts it with the RSA algorithm before storing it. The cloudservice provider authenticates the user's identity before handing over encrypted data that can be unlocked with a personal key.

The three layers of this data security approach all contribute to keeping cloud information safe. Data is authenticated in the first layer, encrypted in the second, and decrypted in the third. If your data is stored in the cloud, RC5 will keep it safe. Theft of encrypted data is catastrophic since no recovery key exists.

With the help of role-based access control (RBAC) cloud architecture and the Role-Based Encryption (RBE) method, businesses can confidently store data in the public cloud while keeping sensitive information about their internal structures in a private cloud.

Data owner, data consumer, cloud server, and N attribute authorities are the four defined authorities in. In order to send encrypted data to a cloud server, the data's owner must first geta public key from the relevant authorities. After receiving a request for information, authorities generate a private key and provide it to the end user. Only once the user has been authenticated by the cloud service will he be able to download the file. There are two distinct approaches to safe cloud computing, one of which necessitates a reliable third party andthe other of which does not. Data stored in the cloud is protected using Elliptic Curve DiffieHellman (ECDH) and symmetric bivariate polynomial-based secret sharing.

In, an encryption method dependent on a user's physical location was unveiled. Data was encrypted using a geo encryption method and labelled with the firm or employee's name in the cloud and on the user's machine. Data is retrieved using a cloud-based search for a matching label whenever it is required. Information kept in the cloud can be encrypted and signed digitally, as well as using the Diffie-Hellman key exchange and the Advanced Encryption Standard. The authentication, data security, and verification needs are met bythis approach.

➢ *Guidelines:-*

According to the findings of research, 21% of studies use guidelines to guarantee the security of data stored in the cloud. By introducing a new cloud system architecture approach that has three features—separation of software service providers and infrastructure service providers, hiding

information about the owner of the data, and data obfuscation—guidelines are provided for data security in the cloud in. In order to guarantee data security in cloud architecture, agents method is introduced. Data security was implemented using three agents:a file agent, an authentication agent, and a key managing agent.

Guidelines for six key data technologies are provided in, including those for protecting data privacy, proving the existence of data and making it usable, trusted access control, retrieving and processing cypher text, controlling access to cloud resources, and trusted cloud computing. In this book, guidelines are given along with a meta-analysis of four different encryption algorithms that can be used to help choosethe best algorithm for a given situation.

- *Framework:-*

14% of the results come from the framework approach. In Trust Cloud, a framework is given that uses a data-centric and detective approach to make data more secure. The goal is to encourage the use of file-centric and data-centric logging mechanisms to make data in cloud computing more secure andprivate. In, a framework is made by building a system with multiple users. The layers of a developed solution are the presentation layer, the business logic layer, and the data accesslayer. The data of users is very safe because of these layers.

In, a framework is given that includes a protocol called Sec Cloud. Sec Cloud is a first protocol that covers secure storage and secure computation in a cloud environment through designated verifier signature, batch authentication, and probabilistic sampling procedures. In the proposed framework,there are three steps. In the first step, data and metadata are indexed to protect against cloud service providers that aren't completely honest. In the second step, encrypted data is given a multi-user, private, keyword-searchable encryption to hide searches and the files that come from them from the cloud service provider. The last step is to use a policy to allow users to share data by using metadata and an encryption scheme.

- *Homomorphic Token:-*

7% of the results come from the homomorphic token scheme. In, homomorphic token scheme is used to protect the security of the data. The proposed plan uses a homomorphic token and checks erasure-coded data in different places. It lets you delete,update, and add data to a data block in a safe and efficient way.By using a homomorphic token scheme with a token pre- computation algorithm, a model from achieves both storage correctness insurance and the identification of a server that is acting up (s).

- *Stripping algorithm, data concealment component, harmonizing and token scheme:-*

The stripping algorithm, data concealment, and harmonising and token scheme each contribute 3%. Stripping protects cloud photo data.The method has three parts: image analysis, data separation, and data distribution. Proposed a design for a data concealment component with three subcomponents: a prediction component, a data generator, anda data marking component, all of which would help keep cloud data safe. The evaluation of this part shows that legitimate users' data is successfully hidden and that they are safe from possible attacks.

A repository that protects privacy was shown in. This repository was mostly focused on harmonising operations to keep data private while keeping harmonising relationships in the cloud. With this plan, the owner of the data will be able to give most tasks that require a lot of computing power to cloud servers without revealing what the data is. To deal with data security in cloud computing, they came up with a good and flexible distribution verification protocol. This protocol checks the integrity of erasure-coded data instead of pseudorandom data by using token precomputation with a sobol sequence. The proposed model has three parts: the distribution of files, the pre-computing of tokens, and the challenge response protocol.

VIII. CONCLUSIONS AND FUTURE DIRECTIONS

Cloud computing is cost-effective, quick to deploy, and accessible. Many practical problems remain, though. One is data privacy. Many researchers contributed to this work to reduce data security issues in this domain. This paper presents a literature review on cloud computing data security. Future plans include exploring other cloud computing security issues and designing a data-concealment encryption model.

ACKNOWLEDGEMENT

I would like to express my very great appreciation to Prof Akanksha Kulkarni of ADYPU for her valuable and constructive suggestions during the planning and developmentof this research work.

REFERENCES

[1]. J. Srinivas, K. Reddy, and A. Qyser, “Cloud Computing Basics,” Build. Infrastruct. Cloud Secur., vol. 1, no. September2011, pp. 3–22, 2014.
[2]. M. A. Vouk, “Cloud computing - Issues, research and implementations,” Proc. Int. Conf. Inf. Technol. Interfaces, ITI,pp. 31–40, 2008.
[3]. P. S. Wooley, “Identifying Cloud Computing Security Risks,” Contin. Educ., vol. 1277, no. February, 2011.
[4]. A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, “An Overview of Cloud Services Adoption Challenges in Higher Education Institutions,” 2015.
[5]. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.
[6]. F. Zhang and H. Chen, “Security-Preserving Live Migration of Virtual Machines in the Cloud,” J. Netw. Syst. Manag., pp. 562–587, 2012.
[7]. J. Hu and A. Klein, “A benchmark of transparent data encryption for migration of web applications in the cloud,” 8thIEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[8]. D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.
[9]. E. Mohamed, "Enhanced data security model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.
[10]. Ajoudanian, Sh., and M. R. Ahmadi. "A Novel Data Security Model for Cloud Computing." *International Journalof Engineering and Technology*, vol. 4, no. 3, IACSIT Press, 2012, pp. 326–29. .
[11]. Kodada, Basappa B., and Demian Antony D'Mello. "Data Security Challenges in Cloud Computing." *Academia Letters*, Academia.edu, July 2021
[12]. Fakhruddin Noori , Abdul Ghafar "Omerkhel", 2021, A Review on Data Security in Cloud Computing, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 03 (March 2021),
[13]. Data Security in Cloud Computing by Ahmed AlbugmiMadini O. Alassafi Robert Walters, Gary Wills
[14]. Rachna, A., and Anshu, P.(Jul-Aug 2013). Secure User Data in Cloud Computing Using Encryption Algorithms in International Journal of Engineering Research and Applications (IJERA), 3(4),1922- 1926.
[15]. Rachna, A., and Anshu, P.(Jul-Aug 2013). Secure User Datain Cloud Computing Using Encryption Algorithms in International Journal of Engineering Research and Applications (IJERA), 3(4),1922- 1926.
[16]. [15] Ko, R. K. L., Kirchberg, M., & Bu Sung, L. (2011, 3-5 Aug. 2011). From system-centric to data-centric logging Accountability, trust & security in cloud computing. Paper presented at the Defense Science Research Conference andExpo (DSR), 2011.
[17]. [16] Gawali, M. B., & Wagh, R. B. (2012, 6-8 Dec. 2012). Enhancement for data security in cloud computing environment. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.
[18]. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., et al. (2014). Security and privacy for storage and computation incloud computing. Information Sciences, 258(0), 371-386.
[19]. Rashid, F., Miri, A., & Woungang, I. (2013, June 28 2013-July 3 2013). Secure Enterprise Data Deduplication inthe Cloud. Paper presented at the Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on.
[20]. [19] Cong, W., Qian, W., Kui, R., & Wenjing, L. (2009, 13-15 July 2009). Ensuring data storage security in Cloud Computing. Paper presented at the Quality of Service, 2009. IWQoS. 17th International Workshop on.
[21]. Tribhuwan, M. R., Bhuyar, V. A., & Pirzade, S. (2010, 16-17 Oct. 2010). Ensuring Data Storage Security in Cloud Computing through Two-Way Handshake Based on Token Management. Paper presented at the Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on.
[22]. Leistikow, R., & Tavangarian, D. (2013, 25-28 March 2013). Secure Picture Data Partitioning for Cloud ComputingServices. Paper presented at the Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on.
[23]. Delettre, C., Boudaoud, K., & Riveill, M. (2011, June 28 2011- July 1 2011). Cloud computing, security and data concealment. Paper presented at the Computers and Communications (ISCC), 2011 IEEE Symposium on. [51] Mishra, R., Dash, S. K., Mishra, D. P., & Tripathy, A. (2011, 8- 10 April 2011). A privacy preserving repository for securing data across the cloud. Paper presented at the Electronics Computer Technology (ICECT), 2011 3rd International Conference on.
[24]. Syam Kumar, P., Subramanian, R., & Thamizh Selvam, D. (2010, 28-30 Oct. 2010). Ensuring data storage security in cloud computing using Sobol Sequence. Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.
[25]. Anane, R., Dhillon, S., & Bordbar, B. (2008). Stateless data concealment for distributed systems. Journal of Computerand System Sciences, 74(2), 243-254.
[26]. An Efficient Approach on Data Security with Cloud Computing Environment: A Comprehensive Research Mrs.Anjali Sharma1 , Dr. Garima Sinha Turkish Journal of Computer and Mathematics EducationVol.12 No.14 (2021), 1372 – 1382
[27]. International Journal of Advanced Research in Computer and Communication Engineering Vol. 10, Issue 7, July 2021 security in cloud computing Mitisha b Barot1, Prof.Riddhi Patel
[28]. International Journal of Engineering Research & Technology(IJERT) ISSN: 2278-0181 Protection and Security of Data in Cloud Computing 1. E. Poonguzhali 2. Suhas Rao M V 3. Shanth GK 4. Mujasem Khanum