Abstract – Cloud computing is an internet-based computing systems where online virtual shared resources are operated by the user as demand on their needs. As modern technology has a vast amount of digital information which can be managed by cloud computing systems so it is a new mechanism to distribute products from producer to consumer in a very different and efficient style of computing. With some advantages of cloud storage system, it has a security flaws in accessing data from another user over the internet. Different types of attack can be done by the third party when sharing file is distributed among the users then there is a chance to attack the sharing files from the unauthorized access. **By distributing sharing access or storage with many other users, it is conceivable for another user to hack their data. This paper discusses the two factor authentications mechanisms for the cloud computing security concerns on shared resources and the way for resolving the security risk on cloud computing devices, resources and the security credentials risk mitigation method or algorithm when a user wants to access a storage system into the cloud.**

I. INTRODUCTION

Cloud computing is a technology term that associates with scalable services, delivering hosted services like accessing, data sharing, processing, etc. over the web on demand basis. It provides an including space for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate branch [1]. Cloud storage typically refers to an object storage services like Google, Microsoft Azure and Amazon S3 Storage. Cloud computing can be defined as the use of new or existing computing hardware and virtualization technologies to form a shared infrastructure that enables web-based value-added services [2]. Depending on the size of business and requirements of infrastructure support for day to day operations, every company needs different services from cloud service provides also individuals will demand services as per their requirements [3]. For example, if a consumer uploads/stores his personnel data such as files, images, videos he can synchronize to other devices from anywhere through some apps or web. An Entrepreneur hosts their apps in the cloud and operate components and services from cloud service providers, such as computing API, Virtual Machines, database, and storage, and so on etc. Cloud computing systems are consisting of large numbers of data manipulations, network, and storage devices across the widely or randomly distributed area and multiple holder can engage on the cloud systems synchronously with different resource requirements. This technology allows access to large amounts of computing power in a virtualized manner by aggregating resources. One of the most recently computing area is named as Big-Data. In that area it is an excessively successful paradigm of service-oriented computing and has revolutionized the way of computing infrastructure is used. Three most popular cloud paradigms include: Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) Figure 1A. The concept however can also be extended to Database as a Service or Storage as a Service. That infrastructure needs to be secure during making cloud computing on storage devices.

Because this outsourcing data storage also can arise the security attack. When a file is distributed locally or broadly over the internet media, then at the same time it has more high security risk that file can be unauthorizedly access by another user, that means, the higher distributions of locations, the more higher risk on accessing data. For example, If Alice wants to share a piece of data (e.g. a video) to Bob but it may be difficult for her to send it by email or message due to the size of data. Instead, Alice uploads the file to a cloud storage system (like google-drive) so that Bob can download it at any time. But in that case if Bob can share this link or data to another user then there is a chance to create a security flaws for authorization to access data but Alice doesn’t know whether bob share his data or not. So, by sharing storage and networks with many other users it is also possible for other unauthorized users to access your data. This action can happen on promising the request from third party users or to do criminal activities on shared access data. Although a user can access this data by giving password or username on the web or app but this method is not suitable for uploading or downloading data from the cloud. As cloud computing systems can be used on large or small-scale organizations but main problem is data is stored at any physical locations. So, the third-party API can easily access to take down the data from these physical locations. In that case a bright solution to secure data on the internet that is encryption decryption technology. Encryption means protecting the data from the unauthorized users through the network communications systems and decryption means at the end user systems, data can be retrieved from network according to a special key. From this encryption-decryption technique even if another user has access the cloud which is encrypted before but he cannot decrypt data because he doesn’t know the encryption decryption key in this network.

|  |
| --- |
|  |
| Figure 1A: Data flow and storage in cloud |

II. ENCRYPTION-DECRYPTION MECHANISMS

REFERENCES

[1] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,”IEEE Transactions on Parallel and Distributed Systems, vol. 27, pp. 340–352, 2016.

[2] Joel Gibson, Darren Eveleigh, Robin Rondeau, Qing Tan,“Benefits and Challenges of Three Cloud Computing Service Models”, 978-1-4673-4794-5/12/$31.00\_c 2012 IEEE”.

[3] G.A.Patil,S. B. Patil, “Data Security Mechanism for Cloud”, International Conference on Emerging Technology Trends (ICETT) 2011 Proceedings published by International Journal of Computer Applications (IJCA), pages 24– 27, 2011