Analytical Approach for Security of Sensitive Business Cloud

Osama Ahmed

***Abstract*— Sensitive cloud storage security is an important part to secure confidential data of business. Sensitive data security in merged cloud database environment increased from few years. Data centers located throughout the world. Providing virtual resources via internet facilitates cloud computing to its consumers. Cloud computing is exciting technology and it can reduce the application cost. This paper conducts the secure all sensitive cloud storage and its solutions. This will helpful the users to know all things are required to be secured when they are planning to protect the cloud storage. Sometime the performance is being compromised of the business and it requires highest security level. This will very helpful for user to appropriate security mechanism choose for the sensitive cloud database according to the business requirements. This paper provide the main concept of security in cloud computing. Security to sensitive data all the four level authentication authorization, data security, network security, cloud security. The growing demand for clouds there is an increasing threat of security becoming a main issue. This paper defines path in which security threats can be a very dangerous to cloud computing and how they can be restricted.**

Keywords: Business Data Security, Network Security, Cloud Security, Security Threats, Secured Cloud Computing.

I. INTRODUCTION

For securing sensitive business data using cloud computing security concern and security risk including its threats, risk, vulnerability. Cloud computing is growing day by day and cloud computing service provider, providing a service such as Infrastructure, Platform and software as a service. Data centers located throughout the world and providing virtual resources via internet to its consumers. Researchers are working on security risks, potential threats, vulnerabilities, and possible countermeasure in enterprise cloud computing constantly [1].

An encryption technique is used for encrypted data in transmission. For secure confidential data like employees information, accounts details, contracts detail, buyer and supplier detail, sales and etc. Decryption techniques are used for get reform original data from cloud storage and properly show through application. Cloud computing is also famous as demand computing. Where information is provided to computer, other devices on request and shared resources. Third party data center provide a solution to user and enterprises with various capabilities to save and process data to storage [2].

Improve security due to centralization of sensitive data. Often security is better or as good as other old traditional security system. Cloud computing is growing day by day and cloud computing service provider, providing a service such as Infrastructure, Platform and software as a service. Cloud is not completely secure or risk-free. Protect system and data security risk management of third party is responsible for taking care.

For securing business sensitive data on cloud computing security concern and security risk including its threats, risk, and vulnerability [3]. Data centers located throughout the world and providing virtual resources via internet to its consumers. Researchers are working on security risks, potential threats, vulnerabilities, and possible countermeasure in enterprise cloud computing constantly. An encryption technique is used for encrypted data in transmission. For secure confidential data like employees information, accounts details, contracts detail, buyer and supplier detail, sales and etc. Decryption techniques are used for get reform original data from cloud storage and properly show through application [4].

II. LITERATURE REVIEW

The Information Technology resources in uses in as a service through a network. The third party provides infrastructure, platform and software as service are available on user requirement. Service level agreement between the customer and provider agreed upon requirement the service type and quality. The Information Technology resources on cloud such as information, application, storage and networks. If application or web based control program installed on local on their computer so it will response very quick. User can access through a web browser. Cloud gives a shared resource of configurable. It's based service level agreements between the consumers and service provider. Cloud Computing Characteristics are as follows [5]:

A user can take any contracted cloud computing resource like storage, service; process and application from a service provider this is call On Demand. Cloud computing services can access from anywhere with supported device through web this is call Network Access. The resources assigned to the customers dynamically depending on the demand. The cloud resource is giving or shared to different customer by a provider. The clouds a resource of a provider is assembled to provide the confined service this is call Resource Pooling [6].

Manuscript Received: 15-05-2018; accepted: 2018; date of current version December- 2018
Osama Ahmed is with Computer information System Department Institute of business management-IOBM, Pakistan (Email: osama.ahmed0082@gmail.com)

A cloud resource is giving to the customer on request when required and after that using it will be release when not required. Resources are unlimited from the view point of a customer's. Only pay for used total resources by customer this is call Rapid Elasticity. Cloud is automatically balance loads and optimizes the use of resources by a user. A user is authorization to monitor and control usage of resources this is calls Measured Service. Cloud Infrastructure the cloud computing has format in two wide points of view to rent the basic structure cloud computing or rent at any special service in cloud computing [7].

The basic infrastructure and cloud service provider is allowing to usage software and hardware on the cloud services with any one soft product or service. Cloud computing is growing day by day and introduces number of terminologies of cloud computing such as Infrastructure, Platform and software as a service. As discussed first in the term of 'cloud computing' is other than a concept, so are the terminologies to describe different composition of cloud computing. Cloud Computing Service Model each one of these layers represents a service model of cloud computing this is called the hypervisor and above this layer of abstraction three layers Infrastructure, Platform and software as service. Infrastructure service model allow access to client with controlled to the virtual infrastructure. This is the bottom level service provide to client. For securing the basic structure client need a senior level experienced network structure engineers. Operating system is the high responsibility to handling anything and especially for the security loads. Some clients declined from this responsibility [8]. From this access user can use OS and installed as on required software. Platform service for all platform pre-installed tools such as compiler in operating system for the clients. Tools are managed by the service provider. This model is such as to the traditional hosting service from a third party like a rent a remote server and development IDE can accessible. In traditional hosting work on manually on user requirement and other hand its works on automatically by the requirement [9].

Software service based on user interface on the application and basic structure and other detail placed on another source it's only accessing by the software service. As usually user access from web browser from computer system or mobile phone apps. Such as Gmail providing an email service and its update by the management not from the user end. User has only access to compose a message, read and deleting option [10].

Cloud Deployment Models three types of cloud deployment models are Private, Public and Hybrid. Private cloud have rights can create such as type of cloud and its controlling, setting and maintaining by the organization. Access available within the company and are managed by the organization [11].

Public cloud giving access to resources dynamically to the Internet using web browser and mobile applications. These type of cloud models are owned by a providers who sales and rent the cloud services. Hybrid cloud is the collection of private and public cloud. This deployment model service is available for both private and public. Providers manage access of both private and public cloud.

Cloud security the web services running on a network structure layer it is able to accessible from the network attackers. If any hackers access the server and down all services, remove or copy sensitive data from the server. The hindering security issue played most important role in cloud computing. No doubt saves your data and running your software on someone else hard disk and us another Operating System appears hard to many. Insecurity issues such as data stolen and loss. Organization's sensitive data and software pose serious threats [12].

Importance of security in cloud, Security is the very important problem which blockage the development of cloud. The idea of sensitive data delivering to other company is serious such that the user needs to be alert in understanding the problem of data violation in this environment. In these basic structure operational and technical counter measures defending against human action is difficult to do malicious or accidental. The internal threat effective way almost every basic structure and remains a problem till date. Cloud access with context of internal cloud resource cans considerably maximum loss to the company for the bad use. These types of attack can disturb maximum number user of cloud. The effect of such attack will be playing a vital role.

Threats in cloud computing major threats explored. Threats are involved in loss and breaches data. Network threats involved in accounts or hijacking service, and API unsafe, malicious internal, insufficient due diligence, not a good use of cloud service and shared technologies risks in cloud environment and some special threats involved in interfaces. Threats in cloud physical and cyber security can be classified which may be risks in cloud computing to cloud computing from traditional computing has a number of security issues. The uninterrupted power supply to natural disasters etc[12]. Carefully maintain safety standards and combustibility global monitoring to prevent security management infrastructure security certificate is provided for holding the property such as data center that deals with the physical properties of the system. He deals with the protection of the cyber world system, the large amount of computing resources in the cloud computing services by users of computing services is not activated during the attacks, which are used to being hit by cyber attacks is. Usually found on many of the attacks are discussed Database service has to fulfill all the characteristics of relational database as well as cloud database. Cloud database is designed for virtualized computer environment. There are two terms used for data storage in cloud DaaS (Data service) & DbaaS (Database service). The relational database server to a cloud deployment as it is not easy. In data as a service only a storage is provided over the cloud to store the data but in database as a service client can store data as well as can run queries over the data to alter them and get some useful information from the cloud database. Cloud database is created from the service provider site. So security should be very high in the cloud database because client has to protect data from the outsider

as well as he has to protect the data from the service provider also. It is possible that the database has some damage from the cloud database provider [13].

Scalability cloud database should be scalable so that it can store data as possible as much when numbers of users in the cloud increases. Heterogeneity cloud database should support all types of users and user can work on various platforms [14].

Confidentiality data should be readable to the valid clients only that is a proper encryption is done to the database so that only authorized user can access data. Cloud not only their own data business perspective, but also consumers and business computing that data is physically stored managing how. Distributed nature of cloud computing services and information and data about ownership alters the many concepts. Some companies in the cloud computing to transform the cloud are stored in third-party service providers, and process such data and their data are of a physical location in the world. This could potentially be a problem. Some sensitive data to the cloud, which will be followed by the organization in another country's privacy laws, is stored in, agree?

The problem of national and international regulatory agencies is necessary for an active and informed role. Some laws and the US -EU Safe Harbor rules in this area have been through the development. Like Amazon providers and customers through local laws, local infrastructure, allowing them to comply with availability zones. The hypervisor or virtual machine level possible risks of attack by cloud vendors used virtual machine technology architecture mythologies are a potential problem. The expansion in the number of virtual machines or creating tremendous potential can be contracted on demand. This technology is hardware and operating system, including virtual machines on site for computer systems of traditional remote version, added [15].

Enterprise environment, authentication and authorization for applications to work with a secure cloud environment may need to be replaced. The proposed models in the literature using two -step verification of the authenticity of the user passwords, smart cards and strong authentication factors like the band is based out of the endorsement. Also a plan attacks against many popular identity management, session key establishment, mutual authentication, provides user privacy and security Cloud storage for business or individual's data is stored in a cloud consists of multiple distributed and accessible to the media. Distribution and integrated resource encryption algorithm provide more secure communications. Statistics "significant" and are only used by the user in the form of scrambled converts the encryption algorithm is the key to decrypt data. Symmetric used for encrypt and decrypt data with only one key for encryption. Another technique using two key private and public keys are known as asymmetric key encryption. Public key encryption is used, and the private key is used for decryption. To implement security in cloud storage use, there is a number of existing techniques [14]. The existing encryption algorithms in use on this research. Uses DES algorithm and RSA algorithm for providing security to cloud storage, in existing systems only one level encryption and decryption is applied to cloud data storage. Cyber criminals can easily cracked one level encryption. Hence we suggested a system which uses multilevel encryption and decryption to provide more security for Cloud Storage [15].

Data breaches secure sensitive or confidential data, copy, move, seen, stolen, deleted and is used by an individual, which is a security risk. Data breach can get financial information such as bank accounts detail, credit card, business accounts, employee information, and personal health information, trade secrets of corporations and clients detail [16].

Cloud computing is an important sensitive information risk management approach to manage risk more effectively capacity. Security updates and new patches can be applied. Security and privacy of sensitive data such as business problems weakness lock cloud computing platform, reliability and performance concerns throughout the world due to the third party data centers being managed [17].

III. METHODOLOGY

a. Method of Security

Applications are not valid normally for suited for cloud infrastructure. For operators to move some applications on cloud basic structure it’s a big challenge. Companies are looking to cost reduction and ability by moving sensitive data. Cloud allow for user to access documents, confidential data on group projects and facilitating cooperation , consumer applications and documents from any location in the world that allows you to access. Cloud providers implemented in the cloud APIs are designed to ensure the safe and must be checked before deploying them. Strong authentication and access control mechanisms to unsafe interfaces and APIs to store data and services should be implemented. Open Web Application Security Project (OWASP) standards and guidelines to help avoid such risks, the application can provide to secure applications. Moreover, the transfer of their data to the cloud provider's Cloud APIs, interfaces and analysis is essential to the customer's responsibility.

b. Authentication Authorization

This requirement should be blocked and unauthorized access to only authorized users can access data and devices is crucial for organizations that. A large number of users access the cloud environment, so these controls are even more important. Enterprise Identity federation and rapid on boarding capabilities with third- party authentication and authorization system should be available to connect.

c. Data Security

Various security measures and techniques to avoid data breach in the clouds have been proposed. Cloud storage feature encryption to protect sensitive data stored in the first with a certain access control policy to encrypt sensitive data can be used. Data in the cloud must be taken to avoid violating certain measures, appropriate access control to prevent unauthorized access; implementing and better prevent

the leakage of sensitive information to know the cloud storage environment risk assessments to make proper isolation between virtual machines to apply the data and its transmission among the various services and networks.

d. Network Security

Data flow on the network to prevent leakage of sensitive information needs to be protected. Thus the Secure Sockets Layer (SSL) and Transport Layer Security for Security (TLS) as the network require the use of encryption techniques. In the case of third -party network sniffing middle layer attacks such as human vital protection against traditional network security issues, port scanning, IP spoofing, packet, etc. The network layer is accessible through SSL encrypt end points with maximum security. End points to ensure that encrypted data in the third- party server and third- party server is transmitted both safe from outside sources, within the third -party server and accessible from the Internet. However, malicious users to sniff network packet network can exploit weaknesses in the security setting.

e. Cloud Security

The protection from these threats can be access only for the authorized person and get by limited hardware and infrastructure. The strong rights control must be implementing by service providers and isolated of data and software management layer functions to only authorized administrators to restrict access. The action of contract, the employee should be part of the behavioral needs of the malicious activity should be taken against anyone involved. Malicious internal encryption of sensitive data storage and public networks can be applied to stop. For organizations fully sensitive data such as key assets before transferring their business and risks associated with the cloud, it is important to understand the scope. Service providers such as firewall logs users and their applications to take measures to protect sensitive data, implement infrastructure must disclose. In addition, the industry standard of using cloud applications and services needs to be established to implement. Cloud data storage providers, and the processing flow after the break to check out some qualitative and quantitative risk assessment methods should perform.

IV. RESULTS & DISCUSSION

The use and convenience, cost, reliability, security and privacy, and the sharing and collaboration Business in the cloud to implement some important results which are given below:

a. Use and convenience

Organization employees regularly work outside the work area and thus having simple to utilize and access to their information. This requirement for workers to approach from remote areas and in addition the expanding number of online exchanges requires a distributed computing arrangement. Bookkeeping and fund work has been outsourced to the cloud, leaving more opportunity for business administrators misuse on key work and activities. Bookkeepers are utilizing cloud advancements for their customers for a helpful month to month expense. The Cloud approach wipes out managerial overhead and licenses access to any area, gadget and from any organization.

b. Cost reduction

Due to the subscription model, there are a huge cost investment funds. The entrance cost for firms using business investigation and knowledge, which needs loads of processing power utilization, has been brought down. Prompt access to equipment and programming assets is accessible with no forthright capital ventures bringing about quicker time to advertise, with IT turn into an operational cost (rather than capital cost). Reception of IaaS lessens capital costs and IT costs. Flexibility in inclining up (adaptable foundation) and discarding the cloud limit when not required is greatly spending inviting. For hazardous plans of action, if the request rises piercingly in the specially appointed way, the versatility of assets gave by Cloud specialist co-ops (operational greatness) turns into a colossal upper hand.

c. Reliability

It is more reliable. Employees can even call up the cloud focus (if necessary) rather than relying upon the in-house IT staff. Information excess is worked in by distributed storage arrangements so the documents are constantly possible, even in the midst of system downtime, control disappointments, and so on. Required unwavering quality level must be seen regardless of low costs of cloud administrations. In it is additionally expressed that fast telephone bolster is required under SLAs by business endeavors giving programmed catastrophe recuperation and move down gives certainty. Endeavors are in progress by the FTC (Federal Trade Commission) and the Cloud Security Alliance to enhance the unwavering quality of these cloud providers.

d. Security and Privacy

Organization discussing cloud security is in reality more worried about having their own particular control (something like a private cloud) than some other difficult issue. Cloud security is great, as dangers get limited because of verification and encryption. Security is uplifted by, for instance, observing exercises, following exchanges, giving specific access to clients, and using solid secret word. Establishment of security patches can be maintained a strategic distance from in these way days and months are spared. There might be some versatility relying upon the cloud arrangement picked; for instance, Google Apps enables certain clients to stipulate the area of information stockpiling to meet the Federal rules. Enhanced security is conceivable because of economies of scale and additionally moderateness of great security specialists. Regardless of whether information security is the fundamental issue for SMBs, despite everything they use open mists, in light of the fact that an open cloud gives standard administrations at sensible cost.

In the past research findings related from cloud computing,

So far main concern is security and they describing about the infrastructure, modal, network layer and threats. Securing sensitive business data and if some organization move the data on cloud so they must need to understand all the mechanism.

V. CONCLUSION

Securing the sensitive database in business involves securing the all the data from every layer. It is not an easy job to provide multiple security levels at each place. When there is the need to secure the confidential data of the business and its employee's personal information and financial details then security must be applied. Sometime the performance is being compromised of the business and it requires highest security level. This will very helpful for user to appropriate security mechanism choose for the sensitive cloud database according to the business requirements. Thus it is the need of securing the database at the four level authentication authorization, data security, network security, cloud security.

So far the cloud computing is not a fully secured still need to be explored. Security is the most important for sensitive business data. Cloud computing security problems associated with security experts are working on. Need a fully protected environment where securely data stored on cloud storage and all layers need to send and get encrypted data transfer to one to another point.

ACKNOWLEDGEMENT

Authors are grateful to the Department of Computer Science and Information Technology, Institute of Business Management (IOBM) Karachi, Pakistan.

REFERENCES

[1] Mariana Carroll, Alta van der Merwe and Paula Kotzé, 2011, Secure Cloud Computing Benefits, Risks and Controls, U.S, pp. 1-2.

[2] C.Lakshmi Devasena, 2014, Impact Study of Cloud Computing On Business Development, Operations Research and Applications: An International Journal (ORAJ), Vol. 1, No.1, pp. 1-2.

[3] Monjur Ahmed and Mohammad Ashraf Hossain, 2014, Cloud Computing and Security Issues In the Cloud, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, pp. 26-27.

[4] Mohammed M. Alani, 2014, Securing the Cloud: Threats, Attacks and Mitigation Techniques, Journal of Advanced Computer Science and Technology, 3 (2), pp. 203-204.

[5] S C Rachana and Dr. H S Guruprasad, 2014, Emerging Security Issues and Challenges in Cloud Computing, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 2, pp. 485.

[6] Raj Kumar, 2015, Research on Cloud Computing Security Threats using Data Transmission, International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, pp. 400.

[7] Atulay Mahajan, Sangeeta Sharma, 2015, The Malicious Insiders Threat in the Cloud, International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, pp. 248.

[8] Muhammad Kazim and Shao Ying Zhu, 2015, A survey on top security threats in cloud computing, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, pp. 109.

[9] Shaik Khaja Mohiddin & Dr.Suresh Babu Yalavarthi, (2015), Research Challenges in the Emerging trends of Cloud Computing, International Journal of Advances in Computer Science and Technology (IJACST), Vol. 4 No.1, pp. 4.

[10] Anjali Nayak & Dr. Sadhna K Mishra, 2015, Cloud Database Security: A Survey, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, pp. 1749-1750.

[11] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang & Anand Ghalsasi, 2011, Cloud computing — The business perspective, Decision Support Systems 51, pp. 183.

[12] Farzad Sabahi, 2012,Secure Virtualization for Cloud Environment Using Hypervisor-based Technology, International Journal of Machine Learning and Computing, Vol. 2, No. 1, pp. 42.

[13] Rashmi, Dr.G.Sahoo & Dr.S.Mehfuz, 2013, Securing Software as a Service Model of Cloud Computing: Issues and Solutions, International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.4, pp. 2.

[14] Shakeeba S. Khan & Prof. R.R. Tuteja, 2015, Security in Cloud Computing using Cryptographic Algorithms, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, pp. 149-151.

[15] Harshal Mahajan & Dr.Nupur Giri, 2014, Threats to Cloud Computing Security, International Journal of Application or Innovation in Engineering & Management (IJAIEM), pp. 1.

[16] Anthony Bisong and Syed (Shawon) M. Rahman, 2011, An Overview Of The Security Concerns In Enterprise Cloud Computing, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, pp. 39.