International Journal of Engineering & Technology, 7 (x) (2018) xxx-xxx

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi:
Research paper, Short communication, Review, Technical paper

CLOUD SECURITY: RISK FACTORS AND SECURITY ISSUES IN CURRENT TRENDS

Dr.K.SAI MANOJ [1]*

[1]CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology, Paritala, AP, India

**E-mail:ceo@innogeecks.com*

Abstract

Now a days, cloud computing is an emerging and way of computing in computer science. Cloud computing is a set of resources and services that are offered by the network or internet. Cloud computing extends various computing techniques like grid computing, distributed computing. Today cloud computing is used in both industrial, research and academic field. Cloud facilitates its users by providing virtual resources via internet. As the field of cloud computing is spreading the new techniques are developing. This increase in cloud computing environment also increases security challenges for cloud developers. Users of cloud save their data in the cloud hence the lack of security in cloud can lose the user's trust.
In this paper we will discuss some of the cloud security issues in various aspects like multi-tenancy, elasticity, reliability, availability etc in various sectors, the paper also discuss existing security techniques and approaches for a secure cloud environment. This paper will enable researchers and professionals to know about different security threats and models and tools proposed.

Keywords*:* Cloud Computing, Cloud Security, Security Threats, Security Techniques, Cloud Security Standards.

1. Introduction

Now a days is a critical requirement to securely storage , managing , sharing and analyze massive, vast amounts of complex data organizing (for example: semi-structured oriented and unstructured oriented) to determine various patterns and trends in proper orderly to improve the high quality of healthcare, much better safeguard the nation and explores alternative different sources of energy. Because of the critical status or nature of their applications, it possibly to important role that clouds environment is secure. The major role on security challenges with clouds is that the authenticated owner of the data may not have control of different sectors where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the various resource memory allocations and scheduling process provided by cloud platforms. Therefore, we need to safeguard the data in the midst of untrusted processes.

Cloud computing is generally known as Internet computing. The general definition of cloud computing was provided by National Institute of Standards and Technology (NIST), USA says that: "Cloud computing is a technical model for enabling on-demand services and user convenient network access to a shared vast of configurable computing resources (for example: Networks operations, Client-servers process, cloud storage applications and their services) that can be rapidly growth provisioned and released with needed minimum management efforts or service provider interaction in existing environment. For another case it is general a paradigm that provides required computing resources and storage while for others it is just a way to access software and data operations from the cloud computing. Now everywhere widely used in Cloud computing, it is popular in organization, scientific, research and academic, defense today because cloud environment provides, its users readability scalability, integrity, reliability, flexibility and availability of data.

Cloud computing also provides reduces the minimal cost by enabling the required sharing of data to the organization/ host industries. Organization or industries can import their data into the cloud so that their shareholders or authenticated user can utilize their data. Apple's apps or Google apps is best an example of cloud computing operation structures. However Cloud computing provides different facilities and benefits, but still it has arises few issues regarding safety access and vast storage of data. Many more issues are there normally related to cloud security as: vendor authenticated lock-in; multi-mode tenancy, loss of control operations, common service disruption, casual data loss etc. are some of the research and development problems in cloud computing. In this paper we analyze the security issues related to cloud computing model and their services, applications. This paper mainly focused on to study different types of attacks and techniques to secure the cloud computing.

Cloud computing characteristics:

2. **On Demand self-service:** A cloud might be an individually attain use computing possibilities, as per the use of various servers, network storing, as on request, without user communicating with cloud provider.
3. **Broad Network Access:** Common services are delivered to across the Internet within a standard mechanism structure and access to the services is possible through assorted customer tools.
4. **Resource pooling:** A multitudinous model is employed to serve various types of users or clients by making possibly pools of various computing resources, as per the request of users these have various existing resources which can be assigned and reassigned dynamically using authenticate ownership.
5. **Rapid Elasticity:** Capabilities might be elastically provisioned or rapidly released. From customers o user view, the service provided possibilities comes out to be within limitless and must have the user or customer capability to purchase or sale in any quantity at any time or any case.

6. **Measured Services:** The provision operation procured by various clients is measurable. The use of asset will be calculated through directed, estimated, and accused for contributor and asset.

2. BACKGROUND

2.1. **Cloud computing:** Cloud computing is rapidly or continuously developing as a standard for sharing and service the data over the remote storage areas in an online cloud server environment. Cloud services offers much better amenities for the valid users or customers to enjoy the on-demand cloud applications without any limits or obligations related to data, during the data retrieving process, various kinds of users may be in a cooperative and associated relationship, and finally data distribution with safely manner becomes important role or aspect.

2.2. **Authentication:** An authenticated user or customer can access its own data item fields, only the authorized partial or entire data fields can be identifies by the legal user through login operations, and any forged or tampered data fields cannot directed by the deceive the valid user or customer.

2.3. **Cloud storage:** Cloud storage means the storage of huge amount of data online in the cloud environment, wherein a company or organization's data is stored in and accessible from multiple possibly distributed operations and connected exiting resources that comprise a cloud computing.

2.4. **Data anonymity:** Any irrelevant small entity cannot recognize the exchanged data and communication state between even it intercepts the exchanged data messages through an open source channel.

2.5. **Forward security:** Any adversary cannot correlate or associate two or more communication sessions to derive the prior interrogations according to the currently continuous captured messages.

2.6. **User/Client privacy:** Any relevant or irrelevant entity cannot know or guess a user's or a client access desire, which represents a client's interest in another client's authorized data fields. If and only if the either clients or users have mutual interests to transfer in each other's authorized valid data fields, the cloud computing server will communicate the two or more clients to realize the valid access permission through sharing operations.

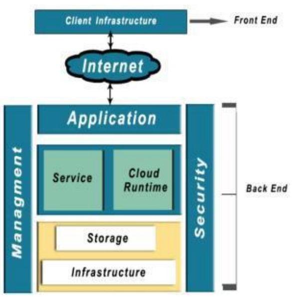

Figure: Cloud computing overview

LITERATURE SURVEY:

Literature survey plays the most key role of step in software development and overview information of entire background work collecting information process. Before developing the required too, it is necessary to determine to identify the time factor, economy strategy of or company or organization strength. Once those possible things are satisfied all necessary requirements, then move next steps are to determine which operating process or system and programming language can be used for developing the existing software tool. Once the programmers or developers can start building blocks of the tool the programmers required to need much amount of external support. This support can be generally obtained from senior technical team leads/peoples or programmers, from technical books or relevant websites. Before building to create the system the above possible consideration are taken necessary action into account for developing various categories of the proposed system.

CLOUD COMPUTING SECURITY ARCHITECTURE:

Cloud Security within surrounding cloud computing is an especially worries few security issue because of the fact that the personal devices used to provide necessary services do not belong to the users or clients themselves. The users have no control of their operations, or any amount of knowledge, what could happen to their data sharing. This is a good effort concern in all cases when clients have valuable and personal authenticated information stored in a cloud computing storage and retrieval service. Users or clients will not compromise their privacy needs, so cloud computing service providers are must ensure that the customer's or clients information is safe manner. This, however, is becoming rapidly challenging various factors because as security levels developments are made in different areas, there always seems to be particular thing identifies to figure out a possible way to disable the security and taken advantage of user information to store secure place. The minimal important components of Service Provider Layer are SLA Monitor, Metering operations, Accounting, Time Scheduling, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, Data traffic controller, retrieval process analyzer and Policy Management. Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity, reliability, association ship and Binding Issues.

Some of the important components or things of Virtual Machine Layer creates much number of virtual machines and number of objective operating systems and its monitoring all operations. Some of the security issues are arises related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, data load failure, Separation between Customers, Cloud security legal and Regularity issues, Identity and Access management operations. Some of the important components or things of Data Center (Infrastructure) Layer contains the IaaS Servers, CPU's, memory management, and storage, and is henceforth typically hypothetically denoted as Infrastructure-as-a-Service (IaaS). Another case security issues related to Data Center Layer are secure data at rest, and Physical Security is combine of Network and Server revival process. Few organizations have been mainly focusing on security leaks and issues in the cloud environment. The Cloud Security Alliance is a non-profit organization creates and, promotes the use of best possible practices for providing security assurance within Cloud Computing, and provides research, organizations, education on the uses of Cloud Computing to help secure all other forms of computing platforms. The Cloud computing - Open Security Architecture (CC-OSA) is another organizations focusing on security issues and risk management.

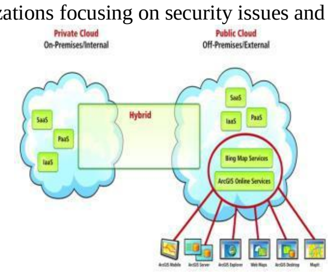

Figure: Cloud computing maping retrieval process

They propose the OSA pattern, which possible pattern is an attempt to illustrate on core cloud functions and operations, the key roles for oversight and risk mitigation, collaboration across various internal organizations through on-demand basis, and the controls all operations that require additional emphasis basis. For example, the security Certification, Accreditation, and Security Assessments series increase in importance role to ensure oversight operations and quality service, assurance given that the operations are being "out-sourced operations" to another service provider. System and Services Acquisition is crucial and critical to ensure that acquisition of quality services is managed reliability manner. Contingency planning stages helps to ensure a close understanding possibility of how to respond in the event of interruptions in existing environment to quality service delivery. The Risk Assessment controls are plays key roles to understand the risks and threats are associated with services in a business or marginal context area. National Institute of Standard and Technology (NIST), USA has initiated and maintains standards, and quality activities to promote standards for cloud computing and alliance branches. To maintain address the risk challenges and to enable cloud computing operations, several standards groups and industry, research consortia are developing on related specifications and test beds.

Some of the existing standards supports and test alliance groups are Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), Storage Networking Industry Association (SNIA) etc. On the another side, a cloud APIs provides either a functional requirement interface or a management interface. Cloud security management has multiple aspects that can be standardized multiple channel for interoperability. Some of the possible standards are Federated security such as identity across clouds, multiple data sets, Metadata and data exchanges among clouds, Standardized outputs for monitoring, auditing, billing, reports and notification for cloud applications and security services, Cloud-independent representation for risk policies and governance etc., below Figure showing the high level view of the cloud computing security architecture.

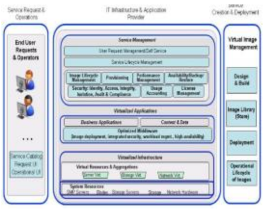

Figure: Cloud computing security architecture

KEY SECURITY ISSUES IN CLOUD COMPUTING:

Cloud computing consists of various applications, platforms and infrastructure segments. Each and every segment performs various operations and offers different software products for businesses and individuals around the technical world. The business cloud application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration and Internet service providers channels. There are numerous security and risk issues for cloud computing as it encompasses many relevant technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, server traffic controls, concurrency control and memory management operations.

Security issues for many kind of these systems and technologies are applicable to cloud computing. For example, the network combines that interconnects between the systems in a public or private cloud has to be secure and mapping possibilities the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate security policies are enforced for data sharing and retrival process. The following below operations are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

3. EXISTING WORK

CLOUD SECURITY ISSUES

Organization or companies are uses various cloud services such as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services has different cloud security issues. Each service model is associated with some security issues. Security issues are considered in two or more views, first in the view of service provider who insures that cloud services provided by them should be secure and also manages the customer's or users identity management. Other view is client or customer view that ensures that security services that they are using is secure path enough.

3.1 **Multi-tenancy:** A cloud based model is built for various reasons such as sharing of resources, memory management, retrival processing, storage and shared computing. Multi-tenancy security provides efficient service utilization of resources, keeping cost lower level. It implies sharing of all computational resources, services storage and cloud applications with other tenants residing on the same logical/physical platforms at provider's premises. Thus it violates the confidentiality of data and results in leakage of information and encryption and increase the possibility of attacks, and reduces the security leaks.

3.2 **Elasticity:** It defines the degree to which a system is able to adapt to the data workload changes by provisioning and deranged existing resources in an autonomic possible manner, such that the available resources matches the current on-demand at any time as closely to as possible too share surrounding resources. Elasticity generally implies scalability, integrity and reliability. It replies that consumers or valid users are able to scale up and down as requirement needed. This scaling enables tenants to use a existing resource that is assigned previously to other equal tenant. In this may lead to confidentiality and risk issues.

3.3 **Insider attacks:** Private Cloud model is a multitenant based objective model that is under the service provider's single management operation domain. This is a view on threat that arises within surrounding the organization. There are no limited hiring standards and providers for cloud employees solve this issues. So a third party vendor can be easily hacking the data of one company or organization and may corrupted or sell that data to any other organization.

3.4 **Outsider attacks**: It is the one of the major attack concerning problem issue in an organization or company because it releases the confidential or secrete information of an organization in open access. Clouds in computing, their not like a private network area, they have more Application Process interfaces than private network. So hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking and easily hacking information from various sources. These attacks are less or minimum harmful than the insider attacks because in the later we sometimes unable to identify the security attack.

3.5 Data Loss: As in any cloud, there are multiple mode tenants, data integrity and safety could not be provided. Data loss can results in financial stage, customer or client count loss for an organization. An important example of this can be updating and deletion of any data without having any backup of that data.

3.6 Network security

- **Man in middle attack**: - In this attack, an attacker makes an independent connection and communicates between the cloud user on its private network where all control is in the hand of attacker.
- **Distributed denial of service attacks**: - In DDOS attack, servers and networks are brought down by a vast amount of network traffic and clients or users are denied the access to a certain Internet based Service operations.
- **Port scanning:** - Port is a place from where information exchange takes place and identifying object verifies virtually. Port scanning is taking place when subscriber configures the group. Port scanning is done automatically when you configure the internet so this violates the security reason concerns.

3.7 Malware Injection Attack Problems

In cloud computing, a vast of data is transferred between cloud service provider and valid client or consumer, there is a need of customer authentication and authorization. When the original data is transferred between cloud service provider and user, attacker can introduce interrupt or malicious code into it. As a possible result, the original valid user may have to wait until the completion of the job that was maliciously introduced.

3.8 Flooding Attack Problem

In cloud computing, there is a no. of qualitative servers that communicate with one another and transfer data. The possible requests is processed, the requested jobs are authenticated initially, but this authentication process requires a vast amount of CPU utilization, memory allocation and finally due to these server side is overloaded and it passes request its offload to other server. By all this the as usual processing of system is interrupted, and the system is flooded automatically.

4. PROPOSED SYSTEM

We are conducting survey and research on secure cloud computing in different factors. Due to the extensive complexity cases of the cloud, we observed contend that it will be difficult to provide a holistic solution to securing problem in the cloud, at present technology strategies. Therefore, our possible goal is to make increment in order enhancements to securing the cloud that will ultimately give result in a secure cloud. In particular case, we are developing a secure cloud environment consisting of hardware (includes 1024TB of data storage on a mechanical non-volatile disk drive, 2400 GB of memory and multiple commodity computers), software (includes Hadoop) and data (a semantic web data repository).

Our cloud system will:

(a) support efficient cloud storage of encrypted sensitive data,
(b) store, manage and query massive amounts of data,
(c) support fine-grained access control
(d) support strong authentication and validation.

In This paper we describe our normal approach to securing environment the cloud. The organization of this paper is as follows: we will give an overview of security issues for cloud storage. We will discuss secure third party authentication of data in clouds. We will discuss how encrypted data may be queried in procedural manner and discuss Hadoop for cloud computing operations and our approach to secure query processes with Hadoop map reducing.

In this paper, we are focusing on some aspects of the secure cloud storage, namely known aspects of the cloud storage and data layers. In particular,

(i) We describe various ways of efficiently storing objects on the data in foreign machines,
(ii) Querying encrypted data, as much of the data on the cloud may be encrypted
(iii) Secure object query processing of the data.

We are using normally Hadoop distributed file system for virtualization at the various storage levels and applying security interfaces for Hadoop which includes an XACML implementation and specifications. In addition ways, we are analyzing and investigating secure federated query processing on different clouds over Hadoop map reduces. These technical efforts will be described in the subsequent adjacent sections.

Security Issues for Clouds

There are numerous security issues for cloud computing as it encompasses many more technologies including such as networks and network alliance technologies, databases, operating systems, Virtual reality, virtualization, resource scheduling, transaction management system, load balancing, data traffic controls, concurrency control, conjunction control and memory management. Therefore, security issues for many of these related systems and technologies are applicable to cloud computing environment. For example, the connected network that interconnects the internal systems in a cloud has to be secure within existing environment. Virtualization paradigm in cloud computing results in many security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

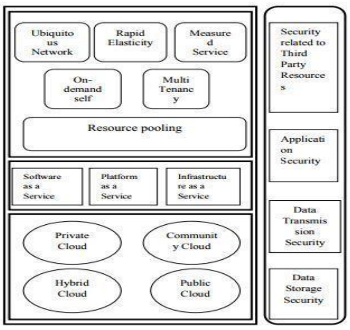

Figure: Complexity of security in cloud security environment

Techniques to secure data in cloud

- **Authentication and Identity**

Authentication of customers or users and even of communicating systems is performed by different methods, but the most of cases used in cryptography technologies. Authentication of customers or clients takes place in different ways like in the form of passwords that is known individually, in the way of a security token, or in the form a various measurable identity quantities such as bio-metric, palm, passwords, eye-iris scan, voice or face recognition, fingerprint. One major problem with using traditional identity way approaches in a cloud computing environment is thoroughly faced, when an organization or enterprise widely uses multiple cloud service providers (CSPs). In such a way use case, synchronizing original identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution.

- **Data Encryption**

If you are planning to store case-sensitive information on a huge data store then we need to use data encryption and decryption techniques. Having passwords and firewalls is good, but people can bypass or hack them to access your data in different ways. When your data is encrypted, it is in a way that cannot be read or access without an encryption security key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key.

- **Information integrity and Privacy**

Cloud computing provides information and resources to valid customers or clients. Resources can be accessed through web browsers or various resources and can also be accessed by malicious attackers in different locations. A convenient solution to the problem of information integrity is to provide mutual trust cases between service provider and valid customer. Another solution can be providing proper channel ways such that security services, authentication, authorization and resources accounting controls, so the process of accessing required information should passes through different multi levels of validation stages to ensure the authorized use of existing resources. Some of the secured access mechanisms should be provided like RSA encrypted certificates, SSH based tunnels, Trusted third party gateways etc..

- **Availability of Information (SLA):** Non availability of information or data is a major issue regarding cloud computing services. Service Level agreement is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and provider [2].An way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability. 3.5 Secure Information Management It is a technique of information security for a collection of data into central repository.

- It is comprised of agents running on systems that are to be monitored and then sends information to a server that is called "Security Console". The security console is managed by admin who is a human being who reviews the information and takes actions in response to any alerts. As the cloud user base, dependency stack increase, the cloud security mechanisms to solve security issues also increase, this makes cloud security management much more complicated. It is also referred as a Log Management.

- Cloud providers also provide some security standards like PCI DSS, SAS 70[2]. Information Security Management Maturity is another model of Information Security Management System. 3.6 Malware-injection attack solution this solution creates a no. of client virtual machines and stores all of them in a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operating systems [10]. The application that is run by a client can be found in FAT table. All the instances are managed and scheduled by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking.

Cloud computing Security Standards

Standards for security define procedure and processes for implementing a security program. To maintain a secure environment, that provides privacy and security some specific steps are performed by applying cloud related activities by these standards.

A concept called "Defence in Depth" is used in cloud to provide security [3]. This concept has layers of defence. In this way, if one of the systems fails, overlapping technique can be used to provide security as it has no single point of failure. Traditionally, endpoints have the technique to maintain security, where access is controlled by user.

- **Security Assertion Markup Language (SAML)**: SAML is basically used in business deals for secure communication between online partners. It is an XML based standard used for authentication, authorization among the partners. SAML defines three roles: the principal (a user), a service provider (SP) and an identity provider (IDP) [3]. SAML provides queries and responses to specify user attributes authorization and authentication information in XML format. The requesting party is an online site that receives security information.

- **Open Authentication (OAuth):** It is a method used for interacting with protected data. It is basically used to provide data access to developers. Users can grant access to information to developers and consumers without sharing of their identity [3]. OAuth does not provide any security by itself in fact it depends on other protocols like SSL to provide security.

- **OpenID** : OpenID is a single-sign-on (SSO) method. It is a common login process that allows user to login once and then use all the participating systems [3]. It does not based on central authorization for authentication of users.

- **SSL/TLS** : TLS is used to provide secure communication over TCP/IP. TLS works in basically three phases: In first phase, negotiation is done between clients to identify which ciphers are used. In second phase, key exchange algorithm is used for authentication [3]. These key exchange algorithms are public key algorithm. The final and third phase involves message encryption and cipher encryption.

SECURITY ISSUES:

The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), and Infrastructure as a service (IaaS). Each service has their own security issues [3]

➢ **Data Security:** Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. Confidentiality is defined as a privacy of data. Confidentiality are designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exist for approved data exchanges. Availability is defined as data is available on time.

➢ **Regulatory Compliance:** Customers are eventually accountable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signaling so these customers can only make usage of paltry operations [11].

➢ **Data Locations:** When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement [9].

➢ **Privileged user access:** Outside the resource data that is processed contains an indigenous risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.

➢ **Trust Issue:** Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

➢ **Data Recovery:** It is defined as the process of restoring data that has been lost, corrupted or accident.

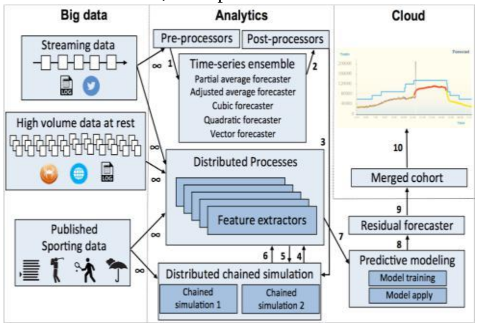

Figure: Data sharing process on cloud environment

Outsourcing: Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owner's control. Massive data and intense computation: Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it i

Use of AES Algorithm:

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, nonlinearity of the key expansion practically eliminates the possibility of equivalent keys in AES.Amongst AES, DES and Triple DES for different microcontroller's comparison is made then it shows that AES has a computer cost of the same order as required for Triple DES [7].

Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blowfish in terms of +time consumption.

Encryption:

A technique is introduced to ensure the availability, integrity and confidentiality of data in cloud by using Secure Socket Layer (SSL) 128 bit encryption that can also be raised to 256 bit encryption. The user who wishes to access the data from cloud is strictly required to provide valid user identity and password before access is given to the encrypted data. In [31], user send the data to the cloud then cloud service provider generate a key and encrypts the user data by using RSA algorithm and stored the data into its data centre. When user request the data from cloud then cloud service provider verify the authenticity of the user and give the encrypted data to the user that can be decrypted by calculating the private key.

In , a three layered data security model is presented in which each layer performs different task to make the data secure in cloud. First layer is responsible for authentication, second layer performs the duty of data encryption and third layer performs the functionality of data recovery. In [33], RC5 algorithm is implemented to secure the data in cloud. An encrypted data is transmitted even if the data is stolen there will be no corresponding key to decrypt the data. In [34] Role Base Encryption (RBE) technique is proposed to secure the data in cloud and role base access control (RBAC) cloud architecture was also proposed which allows organizations to store data securely in public cloud, while maintaining the secret information of organization's structure in private cloud.

In location based encryption technique by using user location and geographical position was introduced. In which a geo encryption algorithm was implemented on the cloud and user computer and the data was labeled with the company name or person who work in the company. When the data is required then in the cloud similar label will be searched and retrieved and the information corresponding to the label will be retrieved. In [38], a technique is proposed by using digital signature and Diffie Hellman key exchange in combination with Advanced Encryption Standard encryption algorithm to protect the confidentiality of data stored in cloud. This scheme is referred as three way mechanism because it provides authentication, data security and verification at the same time.

Strong Authentication

Currently, Hadoop does not authenticate users. This makes it hard to enforce access control for security sensitive applications and makes it easier for malicious users to circumvent file permission checking done by HDFS. To address these issues, the open source community is actively working to integrate Kerberos protocols with Hadoop (Zhang, 2009). On top of the proposed Kerberos protocol, for some assured information applications, there may be a need for adding simple authentication protocols to authenticate with secure co-processors. For this reason, we can add a simple public key infrastructure to our system so that users can independently authenticate with secure coprocessors to retrieve secret keys used for encrypting sensitive data. We can use open source public key infrastructure such as the Open CA PKI implementation for our system (Open CA)..

5. CONCLUSION

This paper we describe some of the cloud security concepts and demonstrate the cloud computing platform properties such as scalability, platform independent, low-cost, elasticity and reliability. Although there are various security challenges in cloud computing but in this paper, we have discussed some of them and also the techniques to prevent them, they can be used to maintain the secure communication and remove the security problems. This survey is basically done to study all the problems like attacks, data loss and unauthenticated access to data and also the methods to remove those problems. As the cloud computing is dynamic and complex, the traditional security solutions provided by cloud environment do not map well to its virtualized environments.

Organization such as Cloud Security Alliance (CSA) and NIST are working on cloud computing security. In this paper we have discussed a few security approaches but several other approaches are also there that are in the process. Some standards are also specified which can be used to maintain secure communication and security in a cloud as many systems communicate in it and perform operations.

Although our review has explored the field, further studies are needed to confirm the obtained results. Future work includes the extension of this review by including more sources (conferences, journals and workshops) and questions. A future plan is to explore the other security issues in the cloud computing environment and we are also aiming to design a security model using some encryption techniques for data concealment in cloud computing..

REFERENCES

[1]. Gates, F., Natkovich, O., Chopra, S., Kamath, S. M., Klamath, P., Narayanamuthry, S. M., et al. (2009). Building a High-Level Dataflow System on top of Map-Reduce: The Pig Experience. In Proceedings of the Thirty-Fifth International Conference on Very Large Data Bases (VLDB) (Industrial, Applications and Experience Track), Lyon, France.

[2]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.376.3145&rep=rep1&type=pdf

[3]. https://www.researchgate.net/profile/Aized_Soofi3/publication/319980773_A_Review_on_Data_Security_in_Cloud_Computing/links/59c8c3e1aca272c71bcd7074/A-Review-on-Data-Security-in-Cloud-Computing.pdf

[4]. http://ieeexplore.ieee.org/document/6848730/

[5]. Hama. (n.d.). Retrieved from http://cwiki.apache. org/labs/cloudsglossary.html

[6].]. Tout, Sverdlik, and Lawver, “Cloud Computing and its Security in Higher Education,” In Proceedings of the Proc ISECON 2009.

[7]. Kant, Dr Chander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 571-575.

[8]. Campbell, Jeronimo, “Applied Virtualization Technology,” Hillsboro, Intel Press (ISBN 09764832-3- 8), 2006, pp. 69-73.

[9]. Dong Xin, et al.”achieving secure and efficient data collaboration in cloud computing. ”Quality of service, 2013 IEEE/ACM 21st International symposium on.IEEE,2013.

[10]. Xia Z., Zhu Y., Sun X. and Chen L. (2014), "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking "Journal of Cloud Computing”,Springer 3.1, pp. 1-11.

[11]. Yunqi Ye, Liangliang Xiao, I-Ling Yen, Farokh Bastani, “Secure, Dependable, and High Performance Cloud Storage”, 2010 29th IEEE International Symposium on Reliable.

[12] A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli,International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11

[13]INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS Dr.Sai Manoj.K International Journal of Current Advanced Research Volume 7; Issue 12(B), December 2018; Page No: 1647316475

[14].Conceptual oriented study on the cloud computing architecture for the fullsecurity Dr.K.Sai Manoj International journal of Engineering and Technology, Volume 7,Issue 4,2018,Scinence Publishing Corporation.

Declarations

Availability of data and material

Not applicable.

Competing interests

Not applicable.

Funding

No funding was applicable.

Authors' contributions

The other of the paper do all the work, the environment for research work are done by my best of my knowledge and supporting my family members.

Acknowledgements

First of all, I am thankful to Honorable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

Authors' information

Dr.K.Sai Manoj CEO Innogeecks Technologies/Amrita Sai Insitute of Science and Technology

,

Dr K Sai Manoj, Founder and Executive Director of Innogeecks Global Services Pvt Ltd, Founder and CEO of Innogeecks Technologies and Founder of 3 start-ups based on IOT and Cloud Computing, is an Enthusiastic learner, Excellent Financial Advisor, Innovative and Visionary Leader, Insightful team builder and strategic planner, who has 10+ years of experience in Financial Services, Equity Research and IT-ITeS services to his credit. He has worked in Reputed Companies like WIPRO Technologies, Fidelity Inverstments.etc.,

He is Proud of achieving many laurels in the field of Computers and Research. He is a Certified Ethical hacker, Certified Computer hacking forensics Investigator, Certified Security Analyst, Charted Engineer from IEI (India), Certified Blockchain Expert, Microsoft Certified Technology Specialist, AWS Certified Solutions Architect-Associate, Google Analytics Individual Qualification, IBM Block chain Certification, Certified EC Council Instructor and so on.

He has a proven record of having 10+ certifications from the most sought after software giants such as Microsoft, IBM, Google, Face book, EC Council & Amazon besides this he has acted as a reviewer for the Journal of Super Computing (Springer) , Journal of Big Data (Springer) and

Journal of the Institution of Engineers (India) – Series B (Springer). And also with his solid financial advice 21 start-ups of Kochi, Bangalore and Vijayawada have tread the success track.

Talking about his research excellence, it is exciting to know that he has filed 3 patents and 4 more are in pipeline and has Published more than 25 research papers in reputed journals like Thomas Reuters, IEEE, Scopus etc., and shows keenness in researching on Cyber Security, Cloud Computing, Big Data / Hadoop, Block chain and Data Analytics