International Journal of Research in Engineering, Science and Management
Volume-2, Issue-12, December-2019
www.ijresm.com | ISSN (Online): 2581-5792

Security in Cloud Computing

B. Rajesh Kumar[1], K. Guna Sekhar[2], M. Charan Kumar[3], K. Hari Kumar[4]
[1]*Assistant Professor, Department of Computer Science and Engineering, Audisankara College of Engineering and Technology, Gudur, India*
[2,3,4]*UG Student, Department of Computer Science and Engineering, Audisankara College of Engineering and Technology, Gudur, India*

***Abstract*: Cloud computing is structure for presenting computing service through the internet on demand and pay according to use get admission to a pool of shared sources particularly networks, garage, servers, services and applications, without physically acquiring them. So it saves dealing with value and time for businesses. Normally information became stored in Relational Databases on one or more servers placed in the business enterprise and the clients had to request statistics from these server machines. This paper presents certain take a look at of IAAS and its additives. "How much secure is cloud computing surroundings?". Noted that security is one of the foremost barrier for continuing increase of cloud computing. For some primary protection risks and troubles corporations and individuals are unwilling to install their data and packages in cloud environment. In this paper, the principle goal is to diagnosed essential security dangers and problems the ones are need to reflect on consideration on for the duration of deployment and improvement of offerings in cloud and the manner how to mitigate those safety dangers and issues. However, it's miles sizeable to recognize that, cloud computing isn't insecure mainly, it just needs to be managed and accessed securely.**

***Keywords*: Cloud computing, Service models, Security risks and issues, Risk mitigation and Cloud services.**

1. Introduction

IT (Information Technology) industries are using technology to a brand new area now and again. The Internet is one of the most famous era now-a-days by the elegance of IT. Now it's far on the edge of revolution, in which assets are globally interconnected. Hence, assets can be easily shared and controlled from everywhere and anytime. Cloud computing is the main element of this widespread, that provides a large garage region where assets are available from anywhere to anyone as a provider in preference to as a product. Throughout in the records of laptop science various tries have been made to release users from the needs of laptop hardware (consisting of storage) and software program, due to the fact that time-sharing utilities estimated in Nineteen Sixties, community computers in Nineteen Nineties and industrial grid computing to cloud computing in greater latest years. Cloud Computing is an allotted architecture that centralizes server resources on a scalable platform in an effort to offer on call for computing assets and offerings. Cloud provider carriers offer cloud systems for his or her clients to apply and create their internet offerings, similar to net provider companies offer cone doubt, Cloud Computing has furnished many exciting services and features like flexibility, reliability, limitless storage, portability and the quick processing strength however cloud security remains a huge trouble. Security troubles including lack of trust, the hazard of malicious insiders, and the failing of cloud services have been mentioned. High speed huge band to get entry to the net.

A. Infrastructure as a service

In IAAS model, Cloud Service Provider outsources storage, servers, hardware, networking components, etc. to the consumer. CSP owns the equipment and responsible for housing, running and maintaining it. In this model, consumer pays on per-use basis. Characteristics and components of IAAS include: Policy-based services

a) Dynamic scaling
b) Automation of administrative tasks
c) Utility computing service and billing model
d) Internet connective
e) Desktop virtualization

B. Background of cloud computing

Cloud computing resulted from the convergence of Grid computing technology. In an early 90's, high overall performance computers have been interconnected via fast statistics communication link to guide complex and clinical calculation. Grid computing defines – a hardware and software program infrastructure that offers steady, pervasive and cheaper get entry to high-end computational centers over communicational network.

C. Cloud Computing

Cloud computing refers to a promising model of computing technology where machines with large data centers can be dynamically provisioned, configured, controlled and reconfigured to deliver services in a scalable manner. It is an innovative IS (Information System) architecture; where visualization as what may be the future of computing "[4]". As being refers to cloud computing, it delivers computing as a service rather than as a product; in which share resources, application software and information to provide computers or other electronic devices as a utility over the Internet in real time.

There is a logical diagram of the cloud computing technologies as shown in Fig. 1.

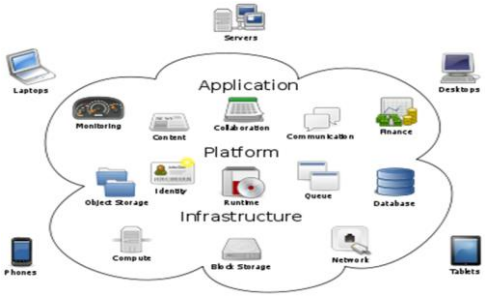

Fig. 1. Cloud computing technologies

In this diagram, cloud computing service models are all inside in the cloud sing and laptops, desktops, phones and tablets are acts like clients to get services from the cloud. Servers provide services to clients according to their request or pay base. Cloud computing provides a shared pool of configurable IT resources on demand, in which needs minimal effort of management to get better services. Services are based on various agreement SLA (Service Level Agreement) between service providers and consumers. There are some key characteristics of cloud computing as follows:

- Application Programming Interface (API) – To enable a machine to interact with cloud software as the same way the interaction between humans/users and computers by using interface services.
- Maintenance – Applications are not necessarily to be installed in each client's system, therefore easy to support maintenance.
- Performance – Web services are constructed by using loosely couple techniques and consistent architectures and monitoring systems to improve services.
- Scalability and Elasticity – Any number of nodes can be added and dropped at any time without much modification of infrastructure and software. A user can get required services without any human interaction. In most cases cloud system scales up automatically.
- Broad Network Access – Cloud services are available over the network, therefore a standard mechanisms are used to provide services on heterogeneous platforms.
- Location Independency – Users are unacquainted about exact location of services except high level of abstraction regard services, such as country, state.
- Reliability – Multiple redundant sites are made for cloud computing environment to support continuity and disaster recovery service for businesses.
- Cost Effectiveness – Centralize infrastructure enables sharing of costs in between large number of users from same or variant locations, such as real estate, electricity (e.g. deployment of cloud services near to the cheap power stations).
- Sustainability – Appropriate resource utilizations for efficient system.
- Security – Due to centralize data center it is possible to improve the level of data security. In present time security is better than the traditional systems, as service providers are able to offer some kind of services to resolve security issues that may not be able to afford by a consumer or a company individually. However, complexity of the security is increased when decentralization of data over the wide area of network and various devices are used to get services. But private deployment model of cloud computing service provides an organization to control information or data security.

D. Platform as a service

Platform as a Service (PAAS) is a manner to lease hardware, working structures, storage and community capacity over an Internet. PAAS is an outgrowth of SAAS that permits hosted software packages to be made available to customer over an Internet. Developer receives many advantages from PAAS. With PAAS, OS can be modified and upgraded as regularly as wanted. PAAS lets in geographically allotted groups to paintings collectively on software program development tasks. CSP have crossed international obstacles for imparting on-going and demanded services to purchasers.

2. Benefits of using cloud computing

Cloud computing provides highly scalable computing environment for an assortment of IT services. It provides services to client individual, to big organizations or companies. As a result, IT departments and individuals are saved application developments, deployments, securities, purchasing new hardware and software and maintenance time and cost effectively. Cloud service helps to reduce power consumption, cooling, storage and uses space for cloud users or consumers in cloud environment. There are two key factors for an organization to concern: Going green and saving charge. In general, most of the benefits are shown based on bar chart in Fig. 2, from most significant to lest significant according to the numbers from 1 to 13.

1.	Cost efficiency	8.	Deployments & change
2.	Scalability	9.	management
3.	Flexibility	10.	Performance
4.	Agility	11.	Mobility
5.	IT Resource management	12.	Automation & supported
6.	and business	13.	management
7.	Efficiency		Security
	Reliability and Availability		Green-IT data center

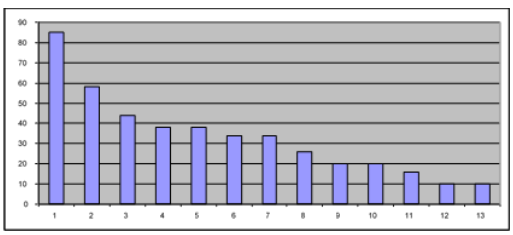

Fig. 2. Benefits

From this chart, it is comprehensible that the main key features to adapt cloud computing to minimize cost efficiently. Other benefits are arranged according to their significant features such as: scalability, flexibility, agility, better IT resource management and business focus, efficiency, higher reliability and availability, rapid development, deployment and change management, better performance and greater mobility. However, it is prominent that, automation improvement, support and management, security and green-IT data centers are the lowest considerable facilities from the survey.

3. Software as a service

Software as a provider every so often known as "software program on demand," is software program that is deployed over an Internet. With SAAS, an issuer licenses a software to clients both as a carrier on demand, thru a subscription, in a "pay-as-you-pass" version, or at no price. This method is the part of the application computing version where all of the generation is within the "cloud" accessed over the Internet as a provider. SAAS turned into first of all broadly deployed for sales pressure automation and Customer Relationship Management (CRM). Now it has come to be common for many commercial enterprise duties, including automatic billing, invoicing, human useful resource management, financials, report control, service desk management and collaboration.

4. Security issues in cloud services

Cloud computing service models are SaaS, PaaS and IaaS, which provides software as a service, platform as a services and infrastructure as a service to end users or customers. These three service models are built on top of each other, as shown in Fig. 3., as a result, their capabilities are inherited as well as security issues and risks.

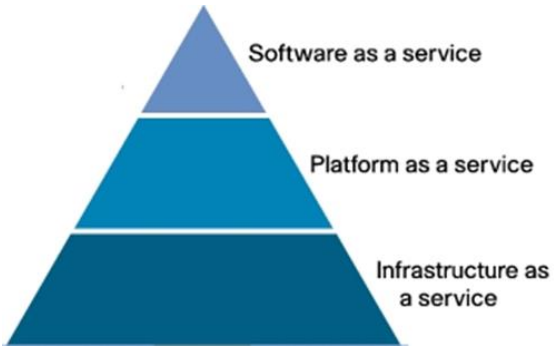

Fig. 3. Cloud computing service models

So, service providers are not be able to take care only part of it, rather than as a whole to provide secure environment. In this part of this paper clearly indicate major security issues based on these service models and what needs to be addressed by implementing appropriate countermeasures.

1) Security issues in SaaS

In time period of SaaS, a customer wishes to depend on the provider carriers for facts safety and carrier vendors must be liable for offering proper safety mechanism to protect information and programs. In this model information is being stored in cloud in conjunction with others groups or people records. The cloud carrier carriers may mirror data in diverse places for facts availability and performance. As a end result, there are some safety problems rise up together with: how is being information saved and in which, what types of protection is being provided for information manipulation and storage. There are a few key safety basics need to be considered for the duration of SaaS deployment and development. There are:

- *Data Security:* When enterprise sensitive data are stored in cloud, vendors should provide physical and logical security, secure access policies and some additional ecurity checks due to security vulnerabilities in applications and concern about malicious employees, who can exploit weakness in data security model. Data control over cloud services make difficult to protect and enforce identity theft and cybercrime security. Sharing resources across multiple domains and failures of data backup also arise some data leakage.
- *Network Security:* In cloud environment data are being transferred over the Internet, thus data flow security is an important issue to avoid leakage of information. To sniff network packets an intruder can make use of data packet to analyze weakness in network security configuration. Attackers can gain access applications and data through hacking such as: some kind of remote access mechanism and injection (SQL and some bad command) vulnerabilities. DoS (Denial of Service), DDoS (Distributed DoS), man in the middle attacks, social networking attacks and some unauthorized attacks creates grate security issues in cloud.
- *Data Confidentiality:* Privacy and confidentiality issues are take placed when data shares between various users, devices and applications. Here multi-tenancy and multitasking (resource sharing and sharing processing resources: CPU- Central Processing Unit) presents a number of confidentiality threats and risks. Data confidentiality in cloud environment related to user authentication. For overall system security software and data confidentiality is also important to prevent unauthorized use of data.
- *Data Integrity:* Data integrity ensures that data are being integral and modified by only authorize entity. Due to increasing number of entities and access points in cloud, authorization becomes crucial that only authorized entities are interact with data. If cloud system resources are not properly segregated among clients then some security issues arise for data integrity. Inadequate encryption and week key management scheme can also lead to security breach.
- *Availability:* Cloud services access on demand by authorized parties even if some authorized entities misbehave or any security breaches. To test

availability of the SaaS vendors, need to consider authentication process and session management weakness issues. Other issues are also need to consider as well such as: data and information service lock in, bandwidth and connectivity speed over the network in cloud services.

- *Data Locality:* In the SaaS model, the consumers are unaware that, where their data is being resided. Some cases it is an issue for some companies for data privacy laws in various countries. So, this service model must be capable of proving data security based on location issues.
- *Access Control:* Many SMB companies store their employees' data in cloud database. The companies have its own policies to access or use data based on their user limitation. So, when an employee left and onboard the SaaS users must bear in mind to enable or disable users account else security breach might be occurred. The SaaS service providers must offer some flexibility to adhere companies' policies in cloud to avoid intrusion of data by unauthorized users.

2) Security issues in PaaS

The primary cause of this model is to guard records. In this model, service provider offers viable command of manipulate together with: OS (Operating System) platform, program development tools and storage area, to construct utility or program on top of provider platform by using the usage of sources. Even although some controls are given to the clients, however nevertheless need to take into account and manipulate a few safety problems beneath the utility degrees together with: community and host intrusion. The service companies must assure in opposition to feasible use of outage and facts remain inaccessible among specific programs. Another thing of security difficulty needs to do not forget that load balancing throughout on systems. The vulnerabilities inside the cloud computing environment are not only related to net related applications but also system to gadget carrier oriented structure programs (SOA). It is referred to that, SOA programs are step by step more deployed in cloud.

3) Security issues in IaaS

Cloud computing combines virtualization technology are innovative manner to provide higher IT services to consumers. Due to growing virtualization generation poses a few safety issues for control over the owner of statistics irrespective of physical vicinity. Various protection problems are get up to installation models in IaaS. Private cloud environment creates fewer protection dangers compared to public cloud. The cloud idea implemented simply over the Internet, so something safety problems and threats are going through inside the Internet, for cloud services need to keep in mind as nicely. Infrastructure isn't always simplest appropriate for hardware resources, where records is being reside or processed, but also the manner statistics are being transmitted over the media from source to vacation spot over the open network. There are some possibilities that information can be routed via intruder's community or infrastructure.

5. Security issues and solution

This section discusses the problems related to cloud computing and their proposed solutions.

1) Trust

Trust between customer and service providers is the main issue faced by cloud computing now days. Customer is never sure whether the Service is trustworthy or not, and whether his data is secure from the intruders or not. The customer and Service provider are bound by Service Level Agreement (SLA) document. This is a type of an agreement between the customer and the service provider; it contains the duties of service provider and his future plans. But unfortunately there are no standards for SLA.

2) Confidentiality

Confidentiality means to prevent the disclosure of private and important information. Since all the information is stored on geographically dispersed locations, confidentiality becomes a big issue. Many methods are used to preserve confidentiality from which, encryption is the widely used method. But it is relatively an expensive method.

3) Authenticity

Integrity is also a main issue faced by cloud computing. It refers to the improper modification of information. As the data resides in different places in a cloud so the access control mechanism should be very secure and each user must be verified as an authentic user. Authentication problem can be solved by using the digital signatures but even after having access to digital signatures a user can't get access and verify the subsets of data.

4) Encryption

Encryption is the most widely used data securing method in cloud computing. It has many drawbacks. It needs high computational power. The encrypted data need to be decrypted every time when a query is run so it reduces the overall database performance. Many methods are presented to ensure better encryption in terms of better security or the operations. A method proposed by suggests that by using several cryptographic methods instead of only one can increase the overall throughput. Data is encrypted using these methods in each cell of a table in cloud. Whenever a user wants to make a query, the query parameters are evaluated against the data stored. The query results are also decrypted by the user not the cloud itself so it increases the overall performance.

5) Key Management

While doing encryption, we need encryption/decryption keys and managing these keys itself is a big security issue in cloud environment. Storing these encryption keys on cloud is a bad option. It is easy to store single encryption key but for the real time systems it become a complex task to store these keys. This may require a separate small database to store the keys locally in a protected database. But again that's not a good idea because

the purpose for which we are shifting our data to clouds will become worthless.

6) Data Splitting

Data splitting may be the better alternative to encryption. It is surely very fast as compared to encryption itself. The main idea behind it is to split the data over multiple hosts that are non-communicable. Whenever a user needs its data back, he must have access to both of the service providers to recollect his original data. No doubt it is very fast technique but it has its own security issues.

6. Conclusion and feature work

One of the biggest security worries with the cloud computing model is the sharing of assets. Cloud carrier providers want to inform their customers on the extent of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security problems and studies challenges in cloud computing. Data safety is major issue for Cloud Computing. There are several other safety demanding situations which includes protection aspects of network and virtualization. This paper has highlighted these types of issues of cloud computing. We consider that due to the complexity of the cloud, it'll be difficult to achieve stop-to-stop security. New protection techniques need to be advanced and older protection techniques needed to be extensively tweaked so as to paintings with the clouds structure. As the development of cloud computing generation continues to be at an early degree, we are hoping our paintings will provide a better expertise of the layout demanding situations of cloud computing, and pave the way for in addition research on this place.

References

[1] Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008.
[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11.
[4] http://www.interoute.com/cloud-article/what-hybrid-cloud
[5] Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computer world.
[6] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance.
[7] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, 2011.
[8] M. Carroll, A. Vander Merwe, P. Kotze, Secure cloud computing: Benefits, risks and controls, Information Security South Africa (ISSA), pp. 1-9, September 2011.
[9] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010.
[10] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2011.
[11] National Institute of Standards and Technology, NIST Cloud Computing Program, 2010. <http://www.nist.gov/itl/cloud/>
[12] Chonka, Y. Xiang, W. Zhou, A. Bonti, Cloud security defence to protect cloud computing against HTTP-DOS and XML-Dos attacks, Journal of Network and Computer Applications, vol. 34, pp. 1097-1107, 2010.
[13] Grobauer, T. Walloschek, E. Stocker, Understanding Cloud Computing Vulnerabilities, Security & Privacy, IEEE, vol. 9, Issue 2, pp. 50-57, March 2011.
[14] B. Thuraisingham, V., Khadilkar, A., Gupta, M., Kantarcioglu, L., Khan, Secure data storage and retrival in the clod, Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on, pp. 1-8, May 2011.
[15] Z., Chen, J., Yoon, IT Auditing to Assure a Secure Cloud Computing, Services (SERVICES-1), 2010 6th World Congress on, pp. 253-259, September 2010.
[16] J., Wayne, T., Grance, Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, January 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf