

Cloud Computing Security Issues and Challenges :- A Survey

Pritam Pravin Shah¹, Prasanna R.Rasal²

Student ¹, MCA-SEM VI, Faculty ² Research Guide, Department of Computer Application, Bharati Vidyapeeth (Deemed To Be University) YM Institute of Management, Karad, India

Abstract - Cloud Computing may be a sort of net based mostly computing which provides services via the web and accesses the resources within the user enterprise either in an exceedingly private-own-cloud or on a third-party server On Demand. The model is characterized by three attributes: quantifiability, pay-per-use, self-services. Many industries like banking, healthcare, Retail, Education, Manufacturing and business are adopting this cloud technique due to potency of services provided by pay-per-use pattern which helps in accessing the networks, storage, servers, services and applications, while not physically getting them. The and Traffic Hijacking

Keywords-Cloud Security; Cloud Computing; Greed Computing

I. INTRODUCTION:-

Cloud Computing has become a compelling force within the world of data Technology. it's thought of in concert of the key options for knowledge storage, security, access, reliable nature on prices. because of the advancement in technology, the usage of net has been raised during a big selection and then the value of the hardware and software system too. so as to abate the value of hardware and software system by providing services once user demands over the web, the cloud computing thought has been winning and gained loads of recognition during a little or no period.

One main reason for the managements to move towards IT is not a new concept, it has recently become a paradigm of solutions is cloud computing ,as they are required to pay the billings for the resources of only how much they consume. Though it distributed computing. In the year 1969, L. Kleinrock predicted that, As of now, computer networks are still in the infancy. But as they grow up and become more sophisticated, we will probably see the spread of computer utilities which, like present electric and telephone utilities, will service individual homes and offices across the country. We now observe, his anticipations were true and are indication of to days utility based computing paradigm. One of most gigantic changes in this world was happened in mid 1990s when grid computing came into existence and provided services on-demand.

The term cloud computing was 1st influenced by Googles business executive Eric statesman in late 2006. From this we will perceive that cloud may be a new development shaped by amalgamating the previous concepts and ideas. Cloud is mostly engineered on grid primarily based design victimization the grid services and different technologies like virtualization and models. the most sanctioning technology of cloud computing is virtualization that separates physical computing devices into 2 or additional virtual devices, in order that it will simply manage the computing tasks. Cloud services area unit provided as major utility services like water, telephone, electricity victimization pay-as-you-use model. These services area unit typically delineate as XaaS wherever X may be something sort of a software package or Infrastructure or platform etc. per the past researches and results, in 2009 , the availability of high-capacity networks, low-cost computers and devices as well as the widespread adoption of hardware Virtualization, Service-Oriented Architecture, Automatic and Utility computing led to a growth in Cloud Computing. In the year 2013 , it was observed that Cloud Computing had become a highly obtained service due to the advantages like High Computing Power, low service costs, scalability, high performance and accessibility.



Fig. Overview of Cloud Computing

II. SECURITY ISSUES IN CLOUD COMPUTING :-

There are various security issues for cloud computing as it comprises of numerous advancements including systems, databases, working frameworks, virtualization, asset planning, exchange administration, stack adjusting, simultaneousness control and memory administration. Similarly, security issues for greater number of these frameworks and technology are pertinent to Cloud computing.

According to the RSA conference which was conducted in the March 2016, the CSA (Cloud Security Alliance) has released the list known as Treacherous 12, which includes the top 12 Cloud Computing threats in 2016. The following are the 12 threats in cloud computing .

- Data Breaches
- Compromised credentials and broken authentication
- Hacked Interfaces and APIs
- Exploited system vulnerabilities
- Account Hijacking
- Malicious Insiders
- The APT parasite
- Permanent data loss
- Inadequate diligence
- Cloud services abuses
- Dos attacks
- Share technology and Share dangers

Data Breaches:

Due to the improved technology, large amount of data is stored in cloud servers, which becomes a target for the hackers. More the amount of data exposed, greater will be the damage to the society and users. The exposure of personal profile would be a normal one, but breaches which involve health information, trading secrets, intellectual property rights would bring a larger destruction. Though Cloud provider typically disposed security controls to protect their environments, it is enterprises which are responsible for securing their own data in cloud. Use of multi-factor authentication and encoding the data or information so that only authorized users can access it.

Compromised Credentials And Broken

Data breaches and other attacks frequently result from slack authentications, weak passwords, poor key or certificate management. Sometimes, not only organizations even we forget to remove the access after our job is done. We can consider for example, the Gmail account if we login in the public accessing places (internet cafes) and forget to logout after our use, exposes our own private data to others. It is our responsibility to remember everything and take care. To avoid these issues, Multi-factor authentications such as one-time passwords, phone-based authentications, OTPs, security questions would make the attacker harder to login from stolen passwords. The rotation of cryptographic keys periodically will not only keep the records secure but also make the resources difficult for the attackers who use keys without authorization.

Hacked Interfaces and APIs

At present, every cloud service provides APIs. They are used to manage the cloud services, management, orchestration, monitoring. The interfaces and APIs which are weak would expose the authorizations to security issues like confidentiality, integrity, availability and accountability. It is recommended by CSA, to focus on threat modeling applications such as architecture/ design which are the primary concepts for the future developments and also to examine the flaws in the security-coding reviews and high level of testing

Exploited System vulnerabilities

We have been facing the problem of bugs since a very longtime. One can say that they are always observed in one or the form. As the usage of technology has increased in a wide range, these vulnerabilities had become a bigger issue. The sharing of memory, data bases and other data among the organizations would lead to data crash or reports larger bugs and later on even may be affected by virus too. To eschew these bugs and system vulnerabilities one may probably have to scan the systems, mobile phones etc. regularly and try to find the solutions for the reported bugs.

III. RESEARCH CHALLENGES IN CLOUD COMPUTING :-

Although cloud computing has quickly come into the existence. The researches of cloud computing are still in an early stage. Many issues have not been resolved and new challenges have been emerging in every industry day-by-day. The following are few research challenges in cloud computing.

- Service level agreement (SLA)
- Cloud data management and security
- Data Encryption
- Virtual machines migration
- Access controls
- Multi-tenancy
- Reliability and availability of services.

Service Level Agreement (SLA):

If needed, many instances of 1 application are replicated on multiple servers on priority basis. Most of the vendors produce SLAs to create a protecting defend against the legal problems, giving minimum assurance to alternative users. Few necessary problems like information protection, outages and value structures are necessary to be thought-about before sign language the contract with the organizations. a number of the all- time queries relating to SLAs are as follows: are the services provided progressing to be ninety nine.9 pace safe? can there be issues like sharing of our personal information throughout the low servers and breakdowns? are they progressing to keep our data? if affirmative, then wherever and the way long? will we have a tendency to get AN assurance that our information are safe with them with none misuse? Is there any SLA that's associating with backup, win and preservation of our data? there's tons of scope and analysis to try to on SLA sand is definitely a very important analysis space in cloud computing.

Cloud Data Management And Security:

Cloud information conception is a vital analysis topic in cloud computing. Cloud information may be an oversized information, unstructured or usually structured with rare cloud updates. The infrastructure supplier, during this context, should reach the objectives like confidentiality, audit ability. Confidentiality is for secure information access whereas transfer and auditability square measure for checking whether or not the arrangement of applications has been altered or not. cryptologic protocols square measure wont to reach the Confidentiality, whereas auditability may be achieved victimization remote attestation techniques. The file systems like GSF and HDSF square measure completely different from ancient distributed file systems particularly in their storage structure, access pattern and application programming interface. because of this, there is also compatibility problems with lasting file, systems and applications. many analysis efforts have studied this drawback

IV. CONCLUSION

Cloud Computing is an emerging technology with a concept of distributed computing. Though it has not come into a full force at present, the future of the software industry is completely going to be dependent on this concept. In this paper, we first discussed about what cloud computing is and Different services provided by Cloud. Later, Importance of cloud computing in key industries, Security issues and research challenges, Applications of cloud computing and future advancements in cloud computing technology. We have observed that here are several security challenges including security aspects of network and virtualization. This paper has highlighted all the security issues in cloud computing and possibly how to avoid them too. New security technologies must be developed and older technologies are needed to be radically tweaked to be able to work with cloud architecture. We believe that Industries are the main sectors for usage of cloud services. The cloud usage in five key industries are studied in this report along with the increase in cloud usage from 2015 to 2017. Last but not least, as whole IT industry is looking forward for the process of Automation, we have provided an overview of how it is going to be with our imagination and what are the basic security issues that are going to be faced in the future. As Automation in Cloud Computing is still an ideal process which needs more clarity and research to be done, we hope that our work will provide a better understanding of design challenges in cloud computing and pave the path for future research in this area.

REFERENCES

- [1]G. O Rabi Prasad, Manas Ranjan, Suresh Chandras Cloud “ Computing: security issues and Research Challenges” published in IRACST-International Journal of Computer Science and Information Technology and Security (IJCSITS), Vol. 1, No. 2, December 2011.
- [2] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I and Zaharia M, “ A view of cloud computing, Communications” of the ACM Magazine , 2010, 53 50-58.
- [3] Ashraf I, “ An over view of service model of cloud computing” published in Int. J. of Multidisciplinary and Current Research, vol.2, 2014, 779-783.
- [4] Bala Narayada Reddy G,” Cloud computing-types of cloud,” 2013, Retrieved from <http://bigdatariding.blogspot.my/2013/10/cloud-computingtypes-of-cloud.html>.
- [5] Christina A A, “ Proactive measures on account hijacking in cloud computing network” published in Asian Journal of Computer Science and Technology, vol.4, 2015, 31-34.
- [6] Choubey R, Dubey R and Bhattacharjee J, “ A survey on cloud computing security challenges and threats” published in International Journal on Computer Science and Engineering (IJCSE), vol.3, 2011, 1227-1231.

[7] Leonard Kleinrock, “ An internet vision: the invisible global infrastructure” published in Ad Hoc Networks, 11, 2003, 1(1):3.

[8] Dinesha H A and Agrawal V K, “ Multi-level authentication technique for accessing cloud services” published in International Journal on Cloud Computing: Services and Architecture (IJCCSA), vol.2, 2012, 31-39.

[9] Doelitzscher F, Sulistio A, Reich C, Kuijs H and Wolf D, “ Private cloud for collaboration and e-Learning services: from I-a-a-S to S-a-a-S” published in J. Computing-Cloud Computing, 2011, 91 23-42.

[10] Hamlen K, Kantarcioglu M, Khan L and Thurai singham B, “ Security issues for cloud computing Optimizing Information Security and Advancing Privacy Assurance: New Technologies” published in International Engineering Research and Innovation

