

Cloud Computing: Elementary Threats and Embellishing Countermeasures for Data security

Ujwal Chopra, Naman Thakur, Lavanya Sharma

Abstract: Internet offers bunch of services and resources, one of them is cloud computing. The centers which provide these services are located all around the world and this service has its own mainstream pros and cons. Cloud computing consists of taking cloud services from the internet and taking them away from the considerable firewall. This paper aims in enhancing specifications of cloud computing, review its security threats and address security concerns along with the cloud operations that needs security. Also, this paper addresses basic security models, qualities and prerequisites for cloud Computing.

Index Terms: Cloud Services, Security model, Prerequisites

I. INTRODUCTION

The way of computing and using its resources have been immensely changed with an intervention of concept of cloud-based computing. The cloud-based computing structure aids with the added benefits that are generally in some other person's consideration or custody and accessed variably by the users pertaining to this system. Ahmed et.al. [1]. Cloud-based computing refers to a technique for conveying Information Technology (IT) advantages in which assets are recovered from the web via on-line applications and apparatuses, rather than a sudden compilation with a server. In contradiction records kept on an exclusive hard disk or drive or nearby stockpiling disk, cloud build capacity makes it easy to conceive to free them to a portable database. The characterizing feature of this method is information being accessed is not depended on the user or his location to be at a particular place to gain accessibility to it and is always found in "cloud". It involves storing files and applications on remote servers and accessing all the data, files and applications using internet [2,5,6,7].

Here, the internet-based storage becomes the storehouse of all the data, files, information and applications which the user can access from anywhere in the world. This system of cloud storage has both pros and cons that have their simultaneous existence in cloud computing world. Cloud computing has been efficiently in use for past few years. The role of cloud-build programs has offered companies with several benefits, in conjunction with the ability to utilize program-based applications from any device, either using an application or a program. Accordingly, users can persist their

data and various files to various devices in a completely feasible way. Storing pictures, files and other relevant data to the cloud frees storage room on the main device of the user. In 2013, Adobe reported every single ensuing form of Photoshop, just as different parts of its Creative Suite, would just be accessible through a web-based membership. This enables clients to download new forms and fixes to their projects effectively.

Precisely, the advantages of cloud computing are enumerated as:

- Allows user to use software from any device, via native app or browser.
- Allows Seamless transfer of files and other important settings of the user from one device to other.
- Allows user to access their emails, on any computers and even storing files using services and resources like dropbox and google drive.
- Has a cost- Saving potential
- Allows users to save their data online as backup files that can be retrieved immediately at the time of hard drive crash or technical failure of device.

At first, security was viewed as a spoiler from utilizing the cloud, particularly when it came to touchy medicinal records and money related data. While guidelines are compelling distributed computing administrations to shore up their security and consistence measures, it remains a continuous issue. Aljazzaf et.al.[5]. Encryption ensures indispensable data, however on the off chance that the encryption key is lost, the information vanishes.

Explained disadvantages of cloud computing are given as follows:

- Downtime: It regularly refers to the most prevalent and substantial disadvantages of cloud-based computing. From a long time, since cloud-based computing relies on web, administration blackouts are dependably an awful probability and can happen in any way, shape or form.[1]
- Privacy and security issues: Preventing data exfiltration, cloud-based computing has its major threat in the terms of securing privacy of data, files and applications of the user.[1]
- Vulnerable to attack: In Cloud-based computing, every component exposes potential vulnerabilities as they are all available online. [1]
- Limited control and Flexibility: Less controlled functions and executed services adds a disadvantage to this system of cloud-based computing. A basic layout of cloud computing as shown in Fig 1 has several components which have their own importance. [1]

Revised Manuscript Received on July 5, 2019.

Ujwal Chopra, Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India.

Naman Thakur, Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh India.

Lavanya Sharma, Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India.

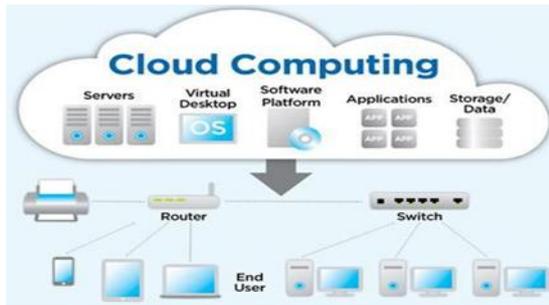


Fig.1. Basic layout of cloud computing [9]

II. RELATED WORK

S.L. Mewada et.al. [2] addressed major security guidelines and principle issues for cloud-based computing along with the advanced summons posed by the new era of cloud computing. He also addressed primary cloud operations and its computational paradigm and security enhancement. Miller[3] discussed fundamentals of cloud computing and describes cloud computing as a web-based application that changes the way of collaboration of entities on-line. Youseff et.al. [4] described establishment of detailed ontology of cloud and cloud-based computing that enabled formation of a better gateway for cloud-based computing platform. Aljazzaf et.al.[5] described the approaches and technologies along with the research issues relevant to cloud computing. It reviews the approaches that quantifies the context of service-oriented architecture of cloud computing. Janesan et.al. [6] overviewed security threats and challenges pertaining to public cloud computing pointing out the sourcing data and files along with applications public to environment of cloud.

S. Subashini [7] surveyed security and threat concerns arising in cloud-based computing due to several cloud computing models. Kraska [8] discussed about web-based database applications on the basis of consistency requirements in context to different infrastructure providers.

III. CHARACTERISTIC FEATURES OF CLOUD-BASED COMPUTING

“Cloud-based Computing is defined as is a model that supports and enhances ubiquitous, suitable, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be provisioned very quickly and further enchanted with minimal management effort or service provider interaction [1]. Various features of Cloud computing are numerated as follows: (as shown in Fig:2).

- Self-service with self-compatibility.
- Functionalities are available all around the globe and can be accessed via standard protocols using different mechanisms by different users.
- The company’s resources are merged and shared to serve multiple customers simultaneously using different virtual resources and dynamics according to customer’s demands.
- Capability can be quickly provisioned to rapidly scale out and scale in.
- Cloud systems control and optimize resource use by

maximally using metering capability at some level of abstraction.

- Easily maintained servers and low downtime
- User can access the data in cloud only by using a compatible device. [10]
- Modification in cloud can be done as per use, it can allow storage usage and allows the customer to buy extra storage if need for a very small amount.
- Economical service where user has to pay for the purchased storage somehow, sometimes very little storage is provided for free also. [10]

Cloud security, has its own importance in these features as It creates a snapshot of the data stored so that the data may not get lost even if one of the servers gets damaged.

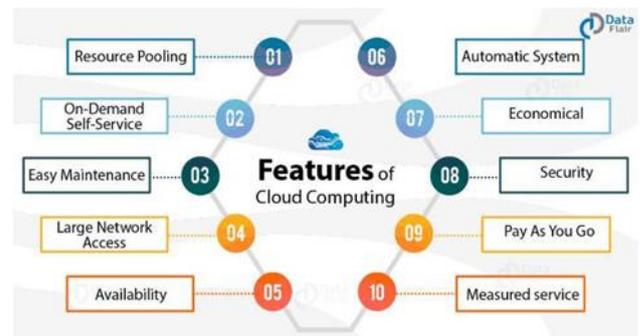


Fig.2.Features of cloud-based computing [10]

IV. VARIANTS OF CLOUD-BASED COMPUTING

The Cloud-based computing is a system, primarily comprising of three services: •software as a service (SaaS) •infrastructure as a service (IaaS) •platform as a service (PaaS). Based on three types of delivery models, the structural layout of cloud-based computing can be kept into three types of delivery models:

- Software as a Service (SaaS): It is a software Distribution model, involving a licensure of software application to the customers. In this, applications are controlled by service providers and are made available to all the customers. It is turning into an undeniably common model showing basic innovations that aid in Service oriented architecture (SOA) and services available on web, develop new formative methodologies wind up well known. Mewada et.al. [1]. Meantime, broadband service has become prevalent to support many user’s access from various areas throughout the globe. [1,2,10,25]
- Infrastructure as a Service (IaaS): It involves systematic delivery system via operating systems from servers and storage using IP based connectivity as procured by an out sourced and on- Demand service. IT resources such as applications, data storing networks are available as a service which are highly standardised and optimized. Customers buy these services with simultaneous addition of customised services on the top of the internal and external use. [1,2,10,25]



There is a high risk of account of the user can get hacked by some undesirable entity by gaining relevant information of the account from the server or other sources. No matter however it is done, it continues to be a major threat to the cloud computing and its users. [1,2]

- Data leakage- The authenticated and highly confidential data of the user stored in the cloud is to major risk for getting leaked either accidentally by the technical failure in the cloud software or deliberately by some undesirable agencies or illegal users commonly known as hackers. [1]

Therefore, this possess another major threat to cloud computing.

- Network attack- Program assaults are regularly utilized in misusing the confirmation and approval vulnerabilities of cloud frameworks today. Malignant assaults and projects, for example, spoofing attacks, ping-of-death assaults, port checking and virus posing dangers to cloud security particularly when actualized by interior or outer cloud clients. [15,16]

- Service hacking- it involves gaining unauthenticated control over authenticated and authorized cloud services by the hackers exploiting software and by performing fraudulent activities. [22]

- SQL-Injection Hacking- It involves hacking of personal data and files along with extraction of sensitive data from the servers of the cloud using special SQL commands and characters, by an unauthenticated and unauthorized SQL expert user. [15]

- Denial of Service attacks- It severely effects the cloud storage availability. It involves accumulating the server with heavy load of data and files, without attending the server's request from other cloud users consequently denying them to provide service. [16]

Apart from these, several other security threats include:

- Cookie poisoning
- CAPTCHA breaking
- Inevitable disclosures of confidential information
- Sniffer attacks
- Cloud challenges inherited from network attacks
- Cross site scripting attacks.

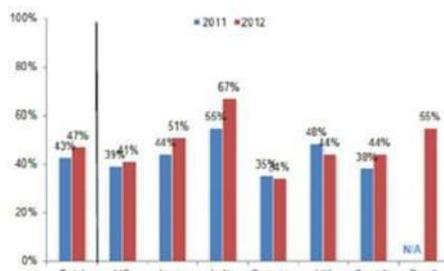


Fig.5. Graphical representation of Data security in different countries around the world [14]

VI. CHALLENGES TO CLOUD COMPUTING

Cloud computing is itself a hub of both advantages as well as disadvantages. Along with these cloud computing also brings numerous challenging aspects (as shown in Fig 6) with itself. Challenges to cloud computing are as follows:

- Security

- Managing cloud spend
- Governance and control
- Compliance
- Managing multiple clouds
- Performance
- Building private cloud



Fig.6. Open Challenging Issues of Cloud Computing [15]

VII. COUNTER MEASURES FOR SECURITY THREATS IN CLOUD COMPUTING

With simultaneous pros, cloud computing has several cons that can adversely lead to disruption in the normal functioning of the cloud system and can leave the users as well as cloud service providing organizations in deep trouble. With the increasing threats, IT world is also preparing itself with the relative countermeasures (as shown in Fig 7), to handle the threats and troubleshoot the related issues. [1,14,15,25]

The countermeasures for these security threats for security related issues in cloud-based computing environment are:

- Data security: with a function of interchanging data and Information within internet premises, large scale exchange systems lead to formation of covert Channels. To regulate information and applications via covert channel, an agent-based security model is designed. [14,15]
- Architecture security: Cloud computing protection demanding situations may be handled almost through appearing safety evaluation. The structural ontology method for secured cloud-based computing is described through Kelvin Jackson. The structure of cloud consists of diverse protection components; security-based API and Network based Security along with Storage based Security. These components fixed in the cloud structure to offer easy and secured cloud computing. [1,25]
- Mirage image management system- Mirage Image, Issues related to secure management of virtual machine images to summarize each application of the cloud are undertaken in this category of software. [1]
- Using client-based privacy manager- its main feature includes making the data hard to read and encode, that automatically reliefs some of the unauthenticated users to access the information and allows simultaneous preference setting to allow users to simultaneously set their preferences to access their personal data.



Module consisting of data access to personal information in the cloud, and the module depicting feedback that manages the feedback of the user regarding the use of his confidential and private data and information. [1, 14,25]

- Transparent cloud protection system- aims in monitoring integrity of cloud components, protecting the integrity of virtual machines, and the distributing computer middleware by permitting host for monitoring guest Virtual machines. [1,3]

Security Issue	Results
Password Recovery	90% are using standard methods like other common services, while 10% are using sophisticated techniques.
Encryption Mechanism	40% are using standard SSL encryption, while 20% are using encryption mechanism but at an extra cost. 40% are using advance methods like HTTPS access also.
Data Location	70% have their datacenters located in more than one country, while 10% are located at a single location. 20% are not open about this issue.
Availability History	In 40% there is a reported downtime alongwith a result in data loss, while in 60% cases data availability is good
Proprietary/Open	Only 10% providers have open mechanism.
Monitoring Services	70% are providing extra monitoring services, while 10% are using automatic techniques. 20 % are not open about this issue.

Fig.7. Preferred measures by Service Providers for the moment [16]

Apart from the above stated measures, some counter-measures for some dangerous type of threats from networking concepts are as listed:

- Sanitizing the consumer input using filtering techniques and many others testing of the SQL injection attacks can be done. An architecture that is proximally false and closer to stopping SQL Injection attacks and simultaneously which detects dynamically and filter out the users' inputs for suspected SQL manage sequences has been proposed. [1,25]
- Actively filtered content, user's data piracy prevention technology, application vulnerability detection technology proposed to prevent XSS attacks. A structure-based guideline that minimises the relativity of the same to the browser for detecting and eliminating untrusted contents are the measures to be taken into consideration. [14]
- These security measures prove to be insufficiently available when the passage within the application sender and a the one who receives gets rerouted through some malevolent connection, instead of using DNS security measures. [1,15]
- Integration of multiple techniques for authenticating CAPTCHA identity (as followed by way of corporations like Facebook, Google etc.) can be an appropriate alternative against CAPTCHA breaking.[15]

VIII. CONCLUSION

With various technologies emerging at a very fast rate, the advancements in conjunction with potentialities to access the cloud services have increased several folds. But along with its utmost acceptable benefits, the cloud-based computing has also been the reason for several web threats. Therefore, a careful analyzation about the efficient uses of cloud computing are to be discussed with counter-measures against the appropriate prevalent threats. This paper aims in enhancing specifications of cloud computing, review its security threats and address security concerns along with the cloud operations that needs security. This paper addresses basic security models; qualities and prerequisites for cloud

Computing. Along with this, cloud models for data security and measures taken in regard to the same are discussed.

REFERENCES

1. M. Ahmed and M.A. Hossain "Cloud Computing And Security Issues In The Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, 2014.
2. S.L. Mewada1, U.K. Singh, P. Sharma "Security Enhancement in Cloud Computing (CC)" Section: Research Paper, Product Type: Isroset-Journal Vol.1, Issue.1, pp.31- 37, Jan-2013.
3. M. Miller, "Cloud Computing-Web Based Application that change the way you collaborate online", Publishing of QUE, 2nd print 2009 [accessed on 28 December, 2018]
4. L. Youseff, S. Barbara "Toward a Unified Ontology of Cloud Computing" [accessed on 25January, 2019]
5. Z.M. Aljazzafa, M.A.M. Capretzb, M; accepted 22 December 2015. [Accessed on 1 February, 2019]
6. W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing" January 2011 [Accessed on 15th February, 2019]
7. S. Subashini, and V. Kavitha "A survey on security issues in service delivery models of cloud computing." J Network Computer Application, Jul, 2010. [Accessed on 20 February, 2019]
8. T. kraska "Building Database Applications in the Cloud", 2010. [Accessed on 3rd March, 2019]
9. Challenges to cloud computing, Available at <https://www.netspaceindia.com/what-is-cloud-computing-how-cloud-managed-services-changing-the-face-of-cloud-hosting-in-india/> [Accessed on: 10-January-2019]
10. Features of Cloud computing, available at <https://data-flair.training/blogs/features-of-cloud-computing/> [Accessed on 10-March-5 2019]
11. Types of cloud computing, available at https://www.researchgate.net/figure/Types-of-Cloud-Computing_fig1_306353636 [Accessed on 20- February- 2019]
12. Types of Cloud computing services, Available at: <http://talkcloudcomputing.com/types-of-cloud-computing-services/> [Accessed on 15- February-2019]
13. Real time applications of cloud computing. Available at https://en.wikipedia.org/wiki/Cloud_computing[Accessed on 14-February-2019]
14. Data security lapse statics in different countries around the world, available at https://www.google.com/search?tbm=isch&q=cloud+computing&chips=q:cloud+computing,g_1:security:clrpWY3VbkU%3D&usg=AI4_-kSuDGHe8FFzvbJY_EnfAuekBhq_nA&sa=X&ved=0ahUKewjeyszNgJbhAhUGS48KHYT4D60Q4IYIKCgA&biw=1242&bih=524&dpr=1.1 [Accessed on 11- February-2019]
15. " Cloud Computing challenging issues" Available at: <https://www.datamation.com/cloud-computing/top-10-cloud-computing-challenges.html> [Accessed on 12-march- 2019]
16. Security Threats and Countermeasures in Cloud Computing available at <https://www.semanticscholar.org/paper/Security-Threats-and-Countermeasures-in-Cloud-Ashktorab-Taghizadeh/4ce891731f0dc7352d329bf2d2cc5b56cb8f6190> [Accessed on 10-February-2019]
18. L.Sharma, N.Lohan, " Internet of Things with Object detection: Challenges, Applications, and Solutions", Handbook of Research on Big Data and the IoT, IGI Global, pp. 89-100, March 2019.
19. L. Sharma, D. Yadav, A. Singh, "Fisher's linear discriminant ratio based threshold for moving human detection in thermal video", Infrared Physics & Technology, Elsevier, vol. 78, pp. 118-128, Sept. 2016.
20. L. Sharma, D. Yadav, "Histogram-based adaptive learning for background modelling: moving object detection in video surveillance", International Journal of Telemedicine and Clinical Practices, Inderscience, vol. 2, no. 1, pp. 74-92, 2017.
21. Lavanya Sharma, Nirvikar Lohan, "Performance analysis of moving object detection using BGS techniques in visual surveillance", International Journal of SpatioTemporal Data Science, Vol.1 No.1, pp.22 – 53, Jan. 2019.

22. BKSP kr. Raju; G. Geethakumari, "A model for trust enhancement in cloud computing", Publisher: IEEE, INSPEC Accession Number: 15022171
23. DOI: 10.1109/ICCCT2.2014.7066716; March, 2015
24. S Abdul S. Muhseen; A.S. Elameer; "A Review in Security Issues and Challenges on Mobile Cloud Computing" (MCC); 2018 1st Annual International Conference on Information and Sciences (AiCIS)
25. Year: 2018; Page s: 133 – 139; IEEE Conferences
26. S.K Gupta; S. Rawat; P. Kumar, "A novel based security architecture of cloud computing; Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization; Year: 2014; Page s: 1 – 6;
27. Cited by: Papers (5); IEEE Conferences
28. B. Gowrigolla; S. Sivaji; M. Roberts Masillamani, "Design and auditing of Cloud computing security" 2010 Fifth International Conference on Information and Automation for Sustainability; Year: 2010; Page s: 292 – 297; Cited by: Papers (8); IEEE Conferences
29. R. Gehlot; N. Sinha; "Enhancing security on cloud using additional encrypted parameter for public authentication", 2016 Symposium on Colossal Data Analysis and Networking (CDAN); Year: 2016; Page s: 1 – 5; Cited by: Papers (3); IEEE Conferences

AUTHORS PROFILE



Ujwal Chopra is an BCA graduate in the field of information technology from Amity University. He is a recipient of several prestigious awards during academic career. He had worked in Catus Technologies Pvt. Limited. He also developed an android application named Indo Tour. He has adequate knowledge of different computer related programming language. His current research interest includes Artificial intelligence and Ethical Hacking.



Naman Thakur is an BCA graduate in the field of information technology. He is a recipient of several prestigious awards during academic career. He had worked in Aspekto digital Pvt. Limited. He also developed a web application named dynamic pole using flask. He has adequate knowledge of different computer related programming language. His current research interests include Cyber Security and Artificial Intelligence.



Dr. Lavanya Sharma is a Ph.D. graduate in the domain of Computer Vision at Uttarakhand Technical University (govt.), India and an assistant professor, Amity Institute of Information Technology at Amity University UP, Noida, India. She is an active nationally recognized researcher who produces dozens of papers in her field. She is an Editorial Member/Reviewer of various journal of repute and active program committee member of various IEEE and Springer conferences also She is an active nationally recognized Computer Vision educator who has produced dozens of papers