iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XII **Month of publication:** December 2020

DOI: https://doi.org/10.22214/ijraset.2020.32504

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XII Dec 2020- Available at www.ijraset.com

Cloud Security at a Glance

Maneesh Pant[1], Praveen Kumar Verma[2], Ravi Kumar[3]
[1]*Department of Computer, Science, College of Engineering Rooree*
[2]*Department of Computer, Science Roorkee Institute of Technology*
[3]*Department of Computer, Science Shri Ram Group of Colleges*

Abstract: ***Advancement in the field of technology have given rise to popularity and growth of cloud computing. As a new paradigm of computing, cloud computing has emerged to change the old ways of computing. The diversity of services delivered through cloud computing model increases their vulnerability to security attacks and incidents. So, the security problem of cloud is very important as it can prevent the rapid development of cloud computing. The main objective of this paper is to highlight the concept of cloud computing and its security risks and challenges. In this paper, we provide an inclusive review of existing security and privacy issues in cloud computing. This paper also surveys the recent research related to cloud security and existing solutions provided in this regard.***

Index Terms- cloud computing, security, data intrusion, service availability, data integrity.

I. INTRODUCTION

Since the introduction of cloud computing, we have various definitions and interpretation of "what is cloud computing". So what exactly is cloud computing? In this regard National Institute of Standards and Technology (NIST) proposed a definition which is most widely recognized and accepted by the researchers. The NIST definition of cloud computing includes virtualized computing resource pool, broad network access, rapid elasticity, on-demand self-service, measured service which comes under the *five essential features;* the *three service models* are *Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) private* cloud, *community* cloud, *public* cloud and *hybrid* cloud comes under the *four deployment models*. It can be shown as in fig.1[1]. The cloud is a metaphor for the Internet, based on how it is described in computer network diagrams, and is a notion for the complex infrastructure it conceals. Cloud Computing is about the delivery of computing resources from a location other than that from the user. As we know that the data storage and computing does not occur in the local computer and server but occurs in all computers distributed in the internet in the cloud computing. The cloud computing move the tasks which are implemented in the personal computer and private data center into the larger computing center which are shared with all users distributed throughout in the internet. It is highly fault tolerant as one service failure will not disrupt other services because it composes applications out of loosely coupled services. The cloud computing system can be divided into two sections: the front end and the back end. They connect to each other through the internet. The front end is user who use the service provided by the back end which is the cloud section of the system. The most important and eye catching feature of cloud computing is its ability to provide on-demand access to a massive repository of recourses such as services, storage, network. These resources can be promptly provided or released with little management effort, since the environment is dynamic and scalable [2].

Cloud computing can deliver a choice of computing infrastructure, software development and deployment platform, or web applications as services, made available to consumers in a pay-as-you-go model. In the industry these services are referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), respectively. [3].

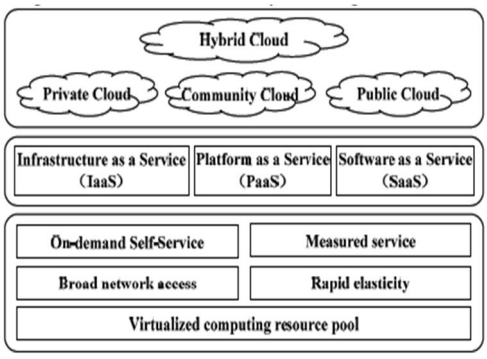


Fig.1. the NIST's definition model of cloud computing[1]

Cloud Security with all its flexibility and dynamic nature have one big concern and that is security. Though cloud is reachingto every field quite rapidly it is still in its early adoption phase. The services provided by cloud needs to be more Dependable, Secure and Relevant. A survey done by IDC took **nine challenges** fig.2 commonly used to evaluate the performance of cloud services and cloud infrastructure. And in that survey security turns up as the major concern. As the information regarding businesses, bank, IT information are very critical in nature customers and end user worry about their vulnerability to attack.

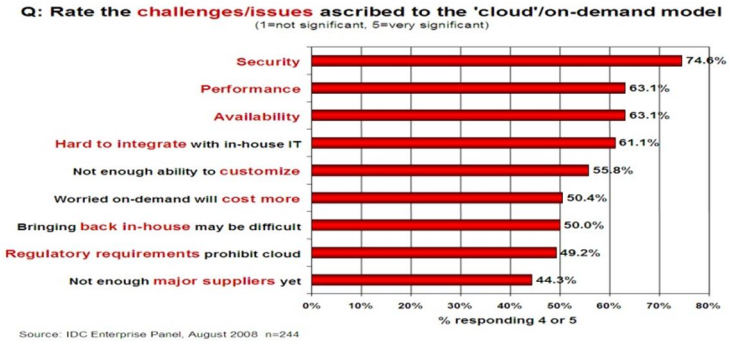


Fig.2 Performance evaluation by IDC

A. Problem Statement

Although cloud computing has been researched earlier, the recent growth in use of cloud services require regular insights into necessary security requirements and its solutions. It is difficult to recognize which kinds of requirements have been researched most and which are – still – under-researched. The objective of this paper is to provide a inclusive and planned overview of the types of security requirements investigated in the area of cloud computing and the proposed solutions to deal with these requirements. This paper thus informs all what is known in published existential studies about security requirements in cloud computing and pinpoints to those types of security requirements that have received much research effort and those that have been under-researched. It moreover addresses and helps developers with a detailed overview to quickly find and address gaps in cloud security issues.

B. Security Requirements in Cloud Computing

In the ISO 7498-2 standard [4], produced by The International Standards Organisation (ISO), Information Security should cover a number of suggested themes. Cloud computing security should also be directed in this regard in order to become a productive and reliable technology solution. Figure 3, illustrating the information security requirements coupled with the Cloud computing deployment model and delivery models has been adapted from Eloff et al [5]. In Figure 3, the different cloud delivery models and deployment models are matched up against the information security requirements with an “” denoting mandatory requirements and an asterisk () denoting optional requirements. However, future work is needed in investigating the optimal balance required in securing Cloud computing. Figure 3 should be viewed in context as a guideline in assessing the security level. Each of the security requirements will be highlighted below in context of Cloud computing.

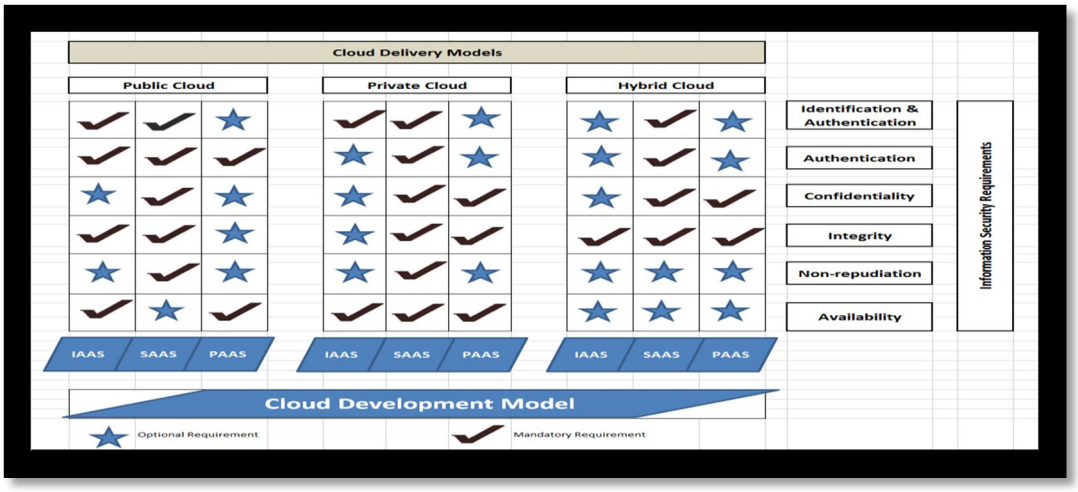


Fig.3. Security Requirements in cloud computing.

C. Security Issues in Cloud Computing

Following are the major issues identified in cloud computing security. These issues are identified with the study of the major work done in the field of cloud computing.

D. Data Security

Security of data inside the cloud infrastructure is a complex issue. The cloud needs to protect the data of government organization, confidential business or data of the various users using the cloud technology as tenants sharing the same infrastructure. Data security gets thwarted when a person who doesn't work in the organization can access your data and can control it. Lack of standards and policies regarding the auditing, compliance, recycling of data i.e. when and what to erase, reporting of data are some of the major concerns.

Wenchao et al. [6] paper of "Towards a Data-centric View of Cloud Security" takes a more data centric approach as mentioned in the title of his paper.

The paper has discussed and explored the secure data sharing among the application hosted on clouds. It discusses the data management issues in distributed query processing,Forensic and system analysis and query correction assurance.

Wenchao proposed Declarative Secure Distributed Systems (DS2) which is a new security platform for cloud computing. The DS2 platform includes the functionality essential for their proposed data security methods. In DS2, the security policies and network protocol are specified Via Secure Network Data log (SeNDlog) a Language which is normally rooted in Datalog that merges logic-based access control Specifications and declarative networking.

By using the Rapid Net declarative networking engine, they have developed the DS2 prototype. The paper supports the distributed Provenance so they have added provenance support to the DS2 platform which according to Wenchaois an important step towards secure cloud data management infrastructure.

The important analysis which concludes the paper is the seamless integration of declarative access control policies, efficient end-to-end verification of data, system analysis and forensics and proposed tool for data centric security which provides secure query processing.

E. Data Integrity

The data integrity in a cloud should be able to preserve the data i.e. it needs to be a secret with its integrity intact. For ensuring data integrity we need to have fine grained access control on data and maintain a single sign in and sign off procedure[7].

F. Data Intrusion

Cloud environment has the similar technology as used in Internet. Therefore, it is open to all the attacks which can be done on the open internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in thecloud.Internetby hackers and cybercriminals needs to be addressedand the cloudenvironment needs to be secure andprivate for clients [8].

[9] Data intrusion can occur in a well build cloud service such as Amazon cloud service. The intrusion can be a hacked password by which the hacker is able to
access all of theaccount's instances and resources. Thus the stolenpassword allows the hacker to erase all the information
inside any virtual machine instance for the stolen useraccount, modify it, or even disable its services.

G. Service Availability

Service availability is going to become a issue for "single cloud" users as there are more chances of service failure.

Service availability is a major issue as mentioned by the big industries of cloud computing such as Amazon. Amazon [10] mentions in its licensingagreement that it is possible that the service might beunavailable from time to time. It is a fact that if a file of any user breaks the cloud storage policy then the user's web service
may terminate for any reason at any time.

In addition, if anydamage occurs to any Amazon web service and theservice fails, in this case there will be no charge to theAmazon Company for this failure.

Backups or use of multiple providers needs to be taken into account by these companies seekingto protect services from such failure [11]. BothGoogle Mail and Hotmail experienced service downtimerecently. If a delay affects payments fromusers for cloud storage, the users may not be able toaccess their data. Due to a system administrator error,45% of stored client data was lost in LinkUp(MediaMax) as a cloud storage provider [12].

H. Quality of service

Quality of service is the measure which guarantees a certain level of output or performance. It can be giving higher or lower priorities to different users, application or services in a cloud environment.

One of the main challenges of Cloud computing is that thesoftware vendor should assume responsibility for maintainingthe application and ensuring quality of service [13].

I. Heterogeneous Environment Management

Heterogeneous environment of cloud possess many advantages like in the dynamic changing environment it can satisfy the high demands of various computational resources in minutes instead of days. In this environment one only pays for what one uses. And after using the resources one can simply release them.

But, it faces security challenges due its heterogeneous nature.[14]The intense of security is directly proportional to the value of the asset it guards. In a cloud where there are heterogeneous systems having a variation in their asset value, a single security system would be too costly for certain applications and if there is less security then the vulnerability factor of some applications like financial and military applications will shoot up. On the other side, if the cloud has a common security methodology in place, it will be a high value asset target for hackers because of the fact that hacking the security system will make the entire cloud vulnerable to attack. In such a scenario, if customized security is provided as a service to applications, it would make sense. Though there are many practical concerns regarding to dynamic security and data storage based on meta-data information my research is much concentrated to derive a framework which targets these concepts and provide a practical solution

J. Examples showing Security Vulnerability of Cloud

1) Example 1 Amazon's server crash raises cloud computing doubts. On the early morning of April 21, 2014 (Pacific Day Time), Amazon's EC2 data center in Virginia crashed, taking down with it several popular websites and small businesses that depend on it. These included favored social networking destinations like Evite, Quora, Reddit and Foursquare, among others[15].

2) Example 2 On 25 April, 2011 thousands of websites, including popular Reddit, still affected 24 hours after the crash started Amazon still suffering server problems Crash leaves firms questioning the future of cloud computing [16].

3) Example 3On May 16,2014 Adobe's ID services went down for over 24 hours, leaving Creative Cloud users -- and a great many others -- locked out of their software and accounts. This isn't the first cloud-related black eye Adobe's suffered, either. Last year Adobe admitted to having 130 million passwords stolen from a backup system that was to have been decommissioned. Many Facebook accounts were also indirectly affected. Adobe's also received sharp criticism for aggressively shepherding its users into cloud subscription, pay-as-you-go plans for its software; in 2013 Adobe stopped selling standalone editions of the Creative Suite altogether [17].

K. Related Work On Cloud Security

We have studied research papers related to security and privacy threats in cloud computing. We searched the addressed security risks that were discussed in those papers and also determined the proposed security mechanisms to address security and privacy in cloud computing. After review we have summarized the following table:

Ref	Year	Addressed security risks			Security Mechanism	Future work/Un addressed issues
		Data integrity	Data intrusion	Service availability		
[18]	2019	✓			Integration of Security and Reputation Approach	The authors propose to implement the proposed model practically on a working cloud environment.
[19]	2019	✓	✓		Security model Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment	For future work author proposed two main research directions first is by adjusting the parameters of the convolutionneural network, the learning ability of the convolution neural network is further optimized and the classification accuracy is improved. Second is game theory is optimized to copewith dynamic changes more dynamically.
[20]	2018	✓	✓	✓	Fast and Parallel Trust computing Scheme Based on Big Data Analysis	Distributed data sharing and remote computing, is a key direction for future research. Another direction is the methodto calculate the trust value of cloud resources with differentvalue of the time window.

[21]	2016	✓	✓		Game Theoretical Approach to Defend Against Co-Resident Attacks	In the future, the author will further consider the impact of thedefense mechanism on normal users, in order to make itas practical as possible. In addition, the current defensemechanism is only for a single datacenter. However, according to the experimental results in [21], the size of a datacenter alsohas an impact on the probability of co-location. Therefore, theywill also investigate how to deploy the defense mechanismacross multiple datacenters, and consider choosing differentdatacenters as one of the attacker's actions.
[22]	2015	✓	✓	✓	Cloud Computing Adoption Framework (CCAF) (Works for Trojan as well)	The authors plan to improve their method and code in the simulation and choose the right type of algorithms to improve the overall performance in execution time of data security and blocking viruses/trojans in real-time.
[23]	2015	✓		✓	Quantitative Reasoning of Cloud Security	As future work, the authors plan extensions to QPT and QHP in order to implement advanced security metrics/Cloud secSLA notions e.g., uncertainty, end-to-end security evaluation (CSP composition), and dependencies within secSLAs elements (e.g., controls, SLOs). The lack of real-world information (including standards and best practices) needed to empirically validate these advanced notions will become an important challenge to overcome e.g., through the CSP community of the Cloud Security Alliance
[24]	2015	✓	✓	✓	Cloud Trust	The scope of initial version of Cloud-Trust is limited to IaaS CCSs and CSPs. It also does not include all possible insider attacks. Potential next steps should be to extend Cloud-Trust to include the full range of insider attacks, and to Platform as a Service (PaaS) and Software as a Service (SaaS) CSPs.
[25]	2014	✓		✓	ISGCloud	It is possible to customize ISGcloud to particular organizations, such as small and medium enterprises that may wish to adopt it but lack the resources of big companies.
[26]	2013	✓	✓		iCloudIDM-LII	Research findings are in progress towards enhancing iCloudIDM-LI and LII with extended features. Inaddition, we are workingtowards architecting iCloudIDM's LIII subsystem to achieve the complete IDM competencies foreCloudIDS architecture.
[27]	2012	✓	✓		Fog computing	The author address the Data security problem of by user profiling but not addresses man in the middle attacks.
[28]	2011	✓			Proposed Two-Tier Security Architecture for Cloud Computing	The framework may also be extended to eradicate data leakages in a heterogeneous cloud computing platform
[29]	2011	✓			Multi shares+ secret sharing algorithm	Multiclouds have received less attention in the area of security.
[30]	2011	✓	✓	✓	DepSky, (Byzantine secret sharing + cryptography)	Authors believe DEPSKY protocols are in an unexplored region of the quorum systems design space and can enable applications sharing critical data (e.g., financial, medical) to benefit from clouds.
[31]	2011	✓			Lucy in the Sky without Diamonds	The paper shows a set of attacks that demonstrate how a malicious insider can easily obtain passwords, cryptographic keys, files and other confidential data.
[32]	2010				RAID-like techniques +introduced RACS	Future research can be done on heterogeneous repositories: Can RACS make use of a desktop PC as one repository, a cloud providers as second, and a cluster as a third? These questions are posed by the paper.

[33]	2010	✓			ICStore,(client centric distributed protocols)	Future work is to implement the proposed model and see its cost and benefits
[34]	2010			✓	SPORC,(fork)	
[35]	2010	Discussions on Cloud Computing Security and architecture			Cloud Computing Roundtable	The authors establishes the fact that, the cloud could well be the biggest botnet. Conversely, of course, we could argue that botnets are the most successful version of cloud computing today.
[36]	2010	Survey paper			Cryptographic Cloud Storage	We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.
[37]	2010	✓		✓	Depot	The authors starts with basic idea“trust no one”. But they fell short of that goal because unless all nodes store a full copy of the data, then nodes must rely on one another for durability and availability.
[38]	2010	✓			Venus	Provides key based security architecture but does not address the group key vulnerability scenario
[39]	2010	Survey Paper			security issues in service delivery models of cloud computing	This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.
[40]	2010				security issues in service delivery models of cloud computing	the issues we’ve discussed here show that existing security and privacy solutions must be critically reevaluated with regard to their appropriateness for clouds. the issues we’ve discussed here show that existing security and privacy solutions must be critically reevaluated with regard to their appropriateness for clouds.
[41]	2010				Impossibility ofPrivacy-Preserving Cloud Computing	The author propose that users of cloud services will also need to rely on other forms of privacy enforcement, such as tamperproof hardware, distributed computing, and complex trust ecosystems.
[42]	2009	✓		✓	HAIL(Proofs +cryptography)	There are a number of interesting HAIL variants to explore in follow-up work. The protocols the authorsdescribed only provide assurance for static files. They have omitted a variant that efficiently accommodates file updates, i.e., small changes to blocks of Files.
[43]	2009	✓			Trusting the cloud	In future we are yet to see how popular storing data in clouds will become, and what protections users will choose to use
[44]	2009	✓			Encrypted cloud VPN	Ensure that you can maintain control of your own virtual server resources with a Virtual Security Gateway so you can enjoy the many benefits of cloud computing while sidestepping the dangers.

Table 1.Related Work on Cloud Computing Security

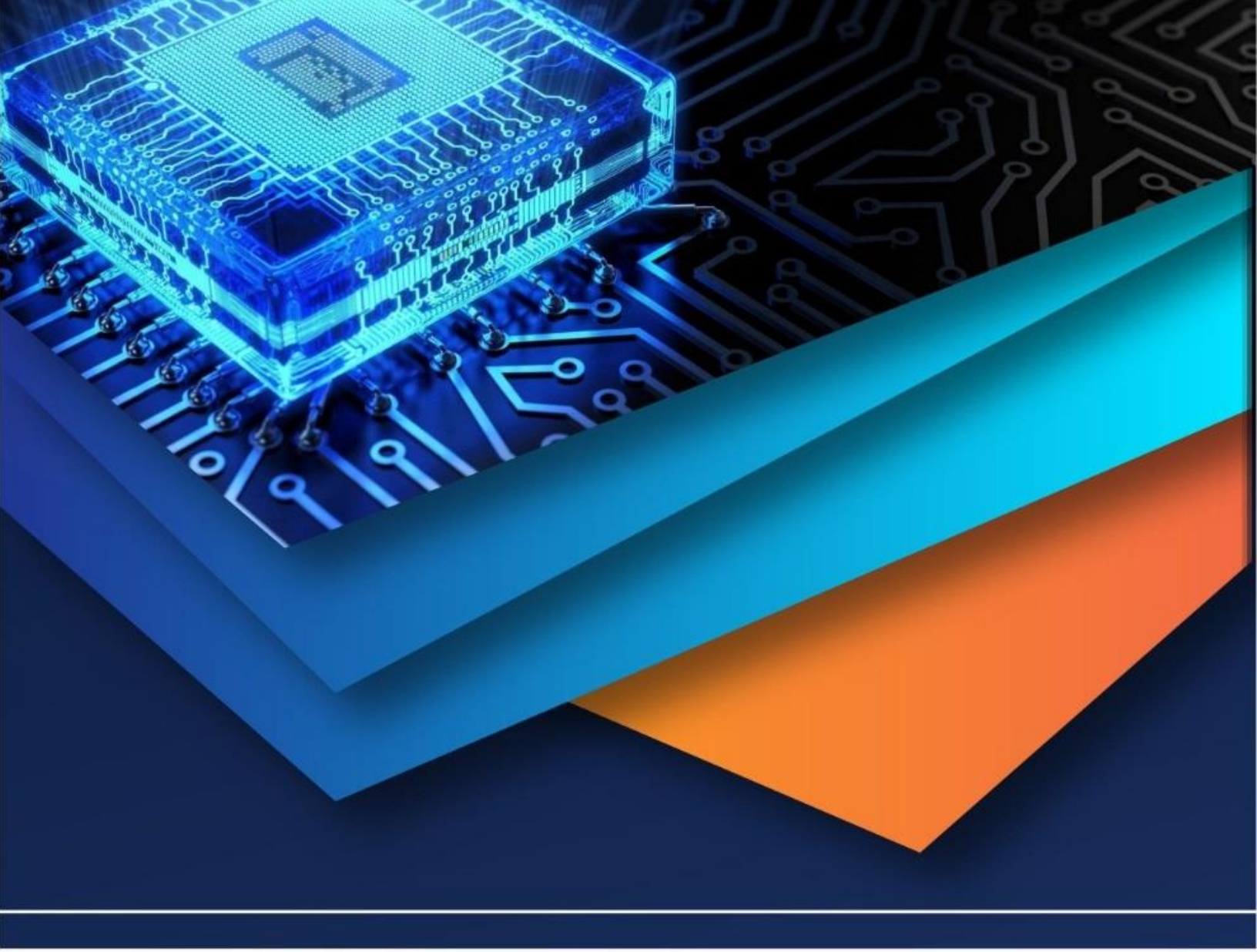
II. CONCLUSIONS

This paper illustrates the concept of cloud computing. Throughout the paper, we havestudied the security and privacy issues in cloud computing. The security challenges faced by cloud providers have been highlighted. We have defined the basic security requirements in cloud model. In this study different security and privacy related research papers were studied briefly. Cloud computing is suffering from a cute security threats. Security is the only worth mentioning weakness of cloud computing.We have identified the major issues in cloud computing security(e.g. data security, data intrusion, data integrity, service availability, quality of service, heterogeneous environment) as well as surveyed the recent research on cloud to address the security risks and solutions. We believe this review will help determine the future research trends in the field of cloud security and privacy.

REFERENCES

[1] Peter Mell, Timothy Grance. The NIST Definition of CloudComputing (Draft).NIST.2011.http://www.productionscale.com/home/2011/8/7/the-nist definition-of-cloud computingdraft.html#axz z1X0xKZRuf.
[2] P. Mell and T. Grance. (2011, May) The nist definition of cloud computing. [Online].Available:http://csrc.nist.gov/publications/nistpubs/800-145/SP800 145.pdflastaccessin28/11/2011
[3] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A breakin the cloud clouds: Towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, January 2009.
[4] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky and D. Shaket, "Venus: Verification for untrusted cloud storage", CCSW'10: Proc. ACM workshop on Cloud computing security workshop, 2010, pp. 19-30.
[5] Takabi, Daniel & Joshi, James & Ahn, Gail-Joon. (2011). Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, IEEE. 8. 24 - 31. 10.1109/MSP.2010.186.
[6] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada
[7] Hwang K. and Li D., "Trusted Cloud Computing withSecure Resources and Data Coloring", IEEE Computing
[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.
[9] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.
[10] Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.
[11] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group,Harvard University, Citeseer, 2007, pp. 1-15
[12] C. Cachin, I. Keidar and A. Shraer, "Trusting thecloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[13] S. Arnold, 2009,' Cloud computing and the issue of privacy', KM World, vol July/August 2008, www.kmworld.com, viewed 19 August 2009, pp 14-22.
[14] A survey on security issues in service delivery models of cloud computing S. Subashini n, V.Kavitha
[15] http://timesofindia.indiatimes.com/tech/it-services/Amazons-server-crash-raises-cloud-computing-doubts/articleshow/8080086.cms
[16] httpwww.dailymail.co.uksciencetecharticle-1381733No-silicon-lining-Amazons-cloud-crash-wipes-customers-data.html
[17] InfoWorld.com, Adobe Creative Cloud crash shows that no cloud is too big to fail
[18] XIANG LI, QIXU WANG, XIAO LAN, XINGSHU CHEN, NING ZHANG and DAJIANG CHEN, "Enhancing Cloud-Based IoT Security Trustworthy Cloud Service: An Integration of Security and Reputation Approach,"2018IEEE Access , doi: 10.1109/ACCESS.2018.2890432,
[19] FANYU KONG, YUFENG ZHOU, BIN XIA, LI PAN AND LIMIN ZHU, "Security Reputation Model for IoT Health Data Using S-AlexNet," 2019 IEEE Access, doi: 10.1109/ACCESS.2019.2950731,
[20] Xiaoyong Li, Jie Yuan, Huadong Ma and Wenbin Yao, "Fast and Parallel Trust Computing Scheme Based on Big Data Analysis For Collaboration Cloud Service,"2018 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 13, NO. 8, AUGUST 2018.
[21] Yi Han, Tansu Alpcan, Jeffrey Chan, Christopher Leckie, and Benjamin I. P. Rubinstein, "GAME THEORETICAL APPROACH TO DEFEND AGAINST CO-RESIDENT ATTACKS IN CLOUD COMPUTING,"2016 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, MARCH 2016.
[22] Victor Chang, Muthu Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework," 2015 IEEE Transactions on Services Computing, doi: 10.1109/TSC.2015.2491281,.
[23] Jesus Luna, Ahmed Taha, Ruben Trapero, and Neeraj Suri, "Quantitative Reasoning About Cloud Security Using Service Level Agreements," 2015 IEEE Transactions on Cloud Computing, doi:10.1109/TCC.2015.2469659.
[24] Dan Gonzales, Jeremy Kaplan, Evan Saltzman, Zev Winkelman and Dulani Woods, "Cloud-Trust - a Security Assessment Modelfor Infrastructure as a Service (IaaS) Clouds," 2015 IEEE TRANSACTIONS ON JOURNAL GONZALES, doi: 10.1109/TCC.2015.2415794.
[25] Oscar Rebollo, Daniel Mellado, and Eduardo Fernandez-Medina, "ISGcloud: a Security GovernanceFramework for Cloud Computing," 2014 The Computer Journal Advance Access, doi::10.1093/comjnl/bxu141
[26] Srinivasan, M.K.Sarukesi, K. ;Revathy, http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=6637432&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6637432
[27] S. J. Stolfo, M. B. Salem and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, 2012, pp. 125-128, doi: 10.1109/SPW.2012.19.
[28] Shantanu Pal, SunirmalKhatua, NabenduChaki,SugataSanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security" http://arxiv.org/abs/1108.4100
[29] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service",44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.
[30] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6th Conf. On Computer systems, 2011, pp. 31-46, https://doi.org/10.1145/2535929
[31] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, 2011, pp. 129-134, doi: 10.1109/DSNW.2011.5958798.
[32] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.
[33] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", IBM Research Report RZ, 3783, 2010.
[34] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp. 1-14.
[35] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud Computing Roundtable," in IEEE Security & Privacy, vol. 8, no. 6, pp. 17-23, Nov.-Dec. 2010, doi: 10.1109/MSP.2010.173.

[36] Kamara S., Lauter K. (2010) Cryptographic Cloud Storage. In: Sion R.et al. (eds) Financial Cryptography and Data Security. FC 2010. Lecture Notes in Computer Science, vol 6054. Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-14992-4_13
[37] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin and M. Walfish, "Depot: Cloud storage with minimal trust", OSDI'10: Proc. of the 9thUSENIX Conf. on Operating systems design and implementation, 2010, pp.1-16.
[38] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky and D. Shaket, "Venus: Verification for untrusted cloud storage", CCSW'10: Proc. ACM workshop on Cloud computing security workshop, 2010, pp. 19-30.
[39] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.
[40] Takabi, Daniel & Joshi, James & Ahn, Gail-Joon. (2011). Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, IEEE. 8. 24 - 31. 10.1109/MSP.2010.186.
[41] Van Dijk, Marten & Juels, Ari. (2010). On the Impossibility of Cryptography Alone For Privacy-Preserving Cloud Computing. IACR Cryptology ePrint Archive. 2010. 305.
[42] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.
[43] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[44] Clavister, "Security in the cloud", Clavister White Paper, 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY