

# A Survey on Cloud Computing and Security Applications

Devarakonda Krishna<sup>1</sup>, S. Malli Babu<sup>2</sup>, D. Prasad<sup>3</sup>

<sup>1,2,3</sup>*Assistant Professor, Department of CSE,*

*St. Martins Engineering College, Hyderabad, India.*

**Abstract:** Cloud computing is a newly evolved technology for complex systems that allow on-demand, flexible, scalable, and low cost services with massive-scale services sharing among plentiful users. The wide receiver of the cloud computing idea has brought about significant effects in both fixed and mobile communication systems prompting frontline research to give fitting System protocols and network architecture, alongside resource administration/management components. In cloud computing, access control and security are two major problems. Therefore, Security of both services and users is a substantial issue for the uses and trust of the cloud computing. This paper audits recent works concentrating on security issues, solutions, and difficulties in cloud computing infrastructure.

**Keywords:** *Cloud Computing, Cloud Security, Cloud Computing Infrastructure, User Authentication.*

## I.INTRODUCTION

Cloud computing is not just a buzz-word, but it represents strong direction of Information Technology industry development. In the last couple of years, "Cloud Computing" has increasingly been discussed. This is a relatively new trend of Information Technology industry development, focused on users, and driven by the increasing use of various mobile devices such as laptops, tablet PCs and smart phones.

Research has shown that it is one of the fastest growing sectors of the digital economy. European governments and industry plan to invest 45 billion Euros in the development of cloud computing by the year 2020. In cloud computing networks of remote servers, storage systems (data centers and server farms) and their resources are being used upon user request.

The term "cloud" is used as a metaphor for the Internet since it doesn't matter where the hardware and software resources that are used are located. For IT professionals cloud computing is a new business model and a new technology platform for developing and deploying applications, and for end-users a new and cheaper way to use applications. Speaking of cloud computing we should be able to distinguish three different models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The scope of this work is a model of Software as a Service.

This represents the lease of computing resources on a network of remote servers where applications are executed and data is stored. The application of cloud computing is very broad and growing daily because of many advantages to the users, and is driven

by the increasing use of various mobile devices (laptops, tablets and smart phones) and mobile Internet access being more available. In general it can be portrayed as a synonym for distributed computing over a network, with the ability to run a program or application on many connected computers at the same time.

It specifically refers to a computing hardware machine or group of computing hardware machines commonly referred as a server connected through a communication network such as the Internet, an intranet, a local area Network (LAN) or wide area Network (WAN) and individual users or user who have permission to access the server can use the server's processing power for their individual computing needs like to run application, store data or any other computing need.

Cloud computing is applicable in education, but it implies the acceptance of these services by all involved in the educational process. Cloud computing provides shared resources, software and information through internet as a PAYGO (Pay-as-you-go) basis. Cloud computing is a kind of virtualization; thus also known as Virtualization Technology.

Cloud computing and its benefits attracts several other field. Education Systems also interacts with educational applications for cloud computing. Cloud computing provides several benefits in educational systems such as creation of virtual teaching learning environment, making interactive and speedy smart classroom. It also minimizes the time of knowledge collection, model preparation and delivery.

Thus, cloud computing has not only many advantages but also some limitations, both arising from the fact that all the data and applications are located somewhere on the Internet. It can be used in various activities of everyday life, including in education. In addition to providing students and teachers (usually fee of charge) access to many applications and services in the cloud, which can be used in formal and informal education, cloud computing allows for greater flexibility and mobility in the use of resources for teaching and learning, greater degree of collaboration, communication and sharing of resources, and creates a personalized learning environment of virtual communities of learning and teaching.

Cloud computing has the potential to offer staff and students better services at a lower cost than the technology deployment models they're using now. Saving money and improving efficiencies are two areas where schools can use all the help they can get. The term, "cloud computing" originated from the clouds metaphor and graphic that are often represent the Internet on network diagrams, because cloud computing relies on applications and file storage that reside on a network, a local area network, a district intranet, or the Internet itself.

## **II. Literature Review**

Nowadays, Cloud computing is a well-known paradigm. However, for the sake of readability and self-containment of the paper, we consider relevant to recap basic notions of Cloud computing. This also allows us to define a common terminology that is going to be used throughout the rest of this paper.

For these reasons, background notions about Cloud computing are provided in this section. NIST defines Cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

Figure 1 depicts the NIST Cloud computing reference architecture. It provides a high-level overview of the Cloud and identifies the main actors and their role in Cloud computing. Each actor is an entity, i.e., a person or an organization, that either takes part in a transaction/process or performs some tasks in Cloud computing. There are five main actors: • Cloud Provider: an entity that provides a service to interested parties; • Cloud Consumer: an entity that uses a service from, and has a business relationship with, one or more Cloud providers; • Cloud Broker: an entity that mediates affairs between Cloud providers and Cloud consumers, and that manages the use, performance, and delivery of Cloud services;

Cloud Carrier: an intermediary that supplies connectivity and delivery of Cloud services from Cloud providers to Cloud consumers;

Cloud Auditor: a party that conducts independent assessments of the Cloud infrastructure, including services, information systems operations, performances, and security of the Cloud implementation.

In terms of interactions, there are several possible scenarios. Generally, a Cloud consumer may request a Cloud service from a Cloud provider, either directly or via a Cloud broker. A Cloud auditor conducts independent audits and may contact other actors to collect the necessary information. The NIST defines the Cloud by means of five essential characteristics, three service models, and four deployment models. Cloud computing is a newly evolved technology for complex systems that allow on-demand, flexible, scalable, and low cost services with massive-scale services sharing among plentiful users. The wide receiver of the cloud computing idea has brought about significant effects in both fixed and mobile communication systems prompting frontline research to give fitting system protocols and network architecture, alongside resource administration/management components. In cloud computing, access control and security are two major problems. Therefore, Security of both services and users is a substantial issue for the uses and trust of the cloud computing. This paper audits recent works concentrating on security issues, solutions, and difficulties in cloud computing infrastructure.

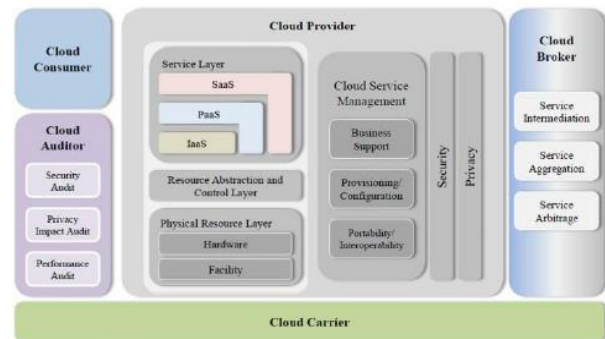


Figure 1. NIST Cloud computing reference architecture.

### III. Cloud Data Security

We have investigated the structure and substance of the system. We attempt to feature the essential improvements and look to future patterns. This investigated goes past simply taking a gander at PC frameworks, cell phones, and different items, and reaches out into expansive ideas like the economy, national security, information assurance, data protection and privacy. Systems to secure again those vulnerabilities are discharged routinely, including for SSL/TLS convention libraries, for example, OpenSSL, however, site proprietors still need to introduce them. We have found that this is still not happening rapidly enough. The quantity of vulnerable websites keeps on persevering a seemingly endless amount of time, with almost no change to appear. While the transfer from SHA-1 certificates to the significantly more grounded SHA-2 is picking up motion, organizations must convey the new testimonies appropriately all together for the progressions to be successful and effective. Immune system for Cloud Computing.

This study takes an abnormal state perspective of Internet threats and cyber security, highlighting the striking changes and progresses. Although, we should not oversee that cyber-crime isn't harmless. For instance, ransom ware keeps individuals out of their PCs, holding treasured family photographs to payment, seizing incomplete original copies for books, and blocking access to government forms, saving money records, and other important reports. In addition, there are no ensures that paying the payoff will discharge those latches.

Organizations, and additionally home users' / clients' have progressed toward becoming casualties, and depending on reinforcements is frequently the last procession of defense when cybersecurity should be the foremost. Directed assaults take valuable intellectual property from the organizations, and an information disruption can scrap an organization's reputation—even devastating its survival. Cyber assurance/insurance claims are rising in number and cost. In the widest sense, cyber security issues debilitate national security and financial development, by which every one of us is influenced.

Any framework is not invulnerable to cybersecurity threats, and in this study, the outcomes of overlooking the dangers from lack of concern, carelessness, and inadequacy is clear. Around three years back a remarkable number of vulnerabilities were recognized, and web assault misuse units are adjusting and advancing them more rapidly than any time in recent memory. As various gadgets are associated, susceptibilities will be misused. Protective Internet-connected gadgets will turn out to be critical to assuring the security of modern control frameworks and medical gadgets in the network. Close by the growing number of software liabilities / vulnerability, and the motorcade of attacks on various frameworks, the future will carry with it a more prominent scope of assorted variety as threats against Windows frameworks will stretch out to other working frameworks, mobile, operating systems and additional IoT devices. The following table consist of various issues, threats and possible solutions for the security threat.

#### **IV. SECURITY APPLICATIONS**

Cloud security applications and SaaS application monitoring solutions are transforming the way enterprises protect against application-layer attacks.

Flaws and vulnerabilities in web applications are one of the primary sources of data breaches, yet only one in 10 enterprises today tests all critical software for resilience against data breaches. Traditional application testing solutions slow the pace of innovation.

Typical on-premises solutions are not only expensive to deploy but complex and time-consuming to operate, creating tension with development teams intent on bringing software to market faster. Consequently, testing is often ignored or postponed until a later date when fixing flaws is more expensive.

Veracode offers a better solution: cloud security applications and cloud-based security testing solutions that are purpose built for the speed and scale required to to simplify secure DevOps and enable development teams to innovate rapidly, Veracode cloud security applications require no special testing expertise and no dedicated staff to operate and maintain. Developers can upload applications to Veracode's online platform and receive test results within a matter of hours. Veracode's cloud security applications combine automated services, centralized policies and world-class expertise to help organizations manage best practices for cloud application security more effectively.

Comprehensive cloud security applications for testing.

Static Analysis, a service that quickly identifies and remediates flaws in any application written, purchased or downloaded.

Software Composition Analysis, a tool for analyzing commercial and open source code and cataloging open source components for greater visibility into risk when open source vulnerabilities are discovered.

Dynamic Analysis, a service that finds, scans and monitors all the web applications belonging to an organization – even the ones that IT teams are unaware of.

Veracode Greenlight, a tool that runs in the background of an IDE to provide developers with real-time feedback and security recommendations as they write code.

#### **V. CONCLUSION**

Cloud computing model can scale up services and virtual assets / resources on request. To process clients traditional cluster system, cloud service gives a considerable measure of points of interest. Cloud computing builds on periods of research in virtualization, scattered figuring, benefit registering, service computing and, all the more as of late, systems administration, and web and software administrations. The cloud is a noteworthy test in how processing of resources will be used since the point of the cloud computing is to alter the financial aspects of the data center, however, before delicate and directed information move into the public cloud. Issues of security benchmarks and similarity must be tended to



including solid verification, secure authentication, assigned authorization, key management for encoded information, data misfortune assurances and regulatory reporting. The clients ought to know about the risks and shortcomings exhibit in the present cloud computing environment before being a part of it. All are components of a protected identity, data and infrastructure model can be connected to the public and private cloud and also to IAAS, SAAS and IAAS services. There is no enormous venture required to update infrastructure, work and proceeding with cost. This paper presented the latest work which is concentrating on security issues, solutions, and difficulties in cloud computing infrastructure. In the advancement of private and public clouds, the specialist service providers should utilize the managing standards to embrace and expand security methods/tools and secure products to create and offer end-to-end dependable cloud computing and services.

## REFERENCES

- [1] K. Yang G, W. Yu, P. ByoungSeob and C. Hyo Hyun, A heuristic resource scheduling scheme in time-constrained networks, *Computers & Electrical Engineering*, Elsevier, 54, 1–15, 2016.
- [2] M. Armbrust, A. Fox, , R. Griffith, A. Joseph, R. Katz, A. Konwinsky, L. Andrew, P. Gunho, A. David, A. Rabkin and I. Stoica, *Above the clouds: a Berkeley view of cloud computing*, University of California at Berkeley, 2009.
- [3] L. Tripathy and R.R. Patra, Scheduling in cloud computing, *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, 4(5), pp.21-7, 2014.
- [4] Wu. Fuhui, Wu. Qingbo and T. Yusong, Workflow scheduling in cloud: a survey, *The Journal of Supercomputing*, Springer, 71, 9, 3373–3418, 2015.
- [5] S. Sing and I. Chana, A survey on resource scheduling in cloud computing: Issues and challenges, *Journal of Grid Computing*, Springer, 14, 2, 217–264, 2016.
- [6] P. Mell and T. Grance, *The NIST definition of cloud computing*, Computer Security Division, Information Technology, Laboratory, National Institute of Standards and Technology, Gaithersburg, 2011.
- [7] P. Patel, A. Ranabahu and A. Sheth, *Service level agreement in cloud computing*, Citeseer, 2009.
- [8] F. Panzieri, O. Babaoglu, S. Ferretti, V. Ghini, and M. Marzolla, *Distributed computing in the 21st century: Some aspects of cloud computing*, Springer, 2011.
- [9] V. Nallur and R. Bahsoon, A decentralized self-adaptation mechanism for service-based applications in the cloud, *Transactions on Software Engineering*, IEEE, 39, 5, 591–612, 2013.
- [10] A. Abdelmaboud, D. Jawawi, I. Ghani, A. Elsafi and B. Kitchenham, ,Quality of service approaches in cloud computing: A systematic mapping study, *Journal of Systems and Software*, Elsevier, 101, 159–179, 2015.
- [11] R. Shelke and R. Rajani, Dynamic resource allocation in cloud computing, *International Journal of Engineering*

Research and Technology, ESRSA, 2, 10, 2013.

[12] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, *Journal of network and computer applications*, Elsevier, 34, 1, 1–11, 2011.

[13] T. Dillon, C. Wu, and E. Chang, Cloud computing: issues and challenges, *International Conference on Advanced Information Networking and Applications*, IEEE, 27–33, 2010.

[14] D. Goutam, A. Verma, N. Agrawal, The performance evaluation of proactive fault tolerant scheme over cloud using CloudSim simulator, *International Conference on the Applications of Digital Information and Web Technologies (ICADIWT)*, IEEE, 171–176, 2014.

[15] S. Ramgovind, M. Eloff, and E. Smith, The management of security in cloud computing, *Information Security for South Africa*, IEEE, 1–7, 2010.

[16] R. Patil and RK. Singh, Scaling in Cloud Computing, *International Journal of Advance Research*, IJOAR, 1, 21–27, ISSN:2320-9194, 2013.

[17] V. Chang, D. Bacigalupo, G. Wills and D. De Roure, A categorisation of cloud computing business models, *Proceedings of the IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, IEEE Computer Society, 509–512, 2010.

[18] M. Petticrew and H. Roberts, *Systematic reviews in the social sciences: A practical guide*, John Wiley & Sons, 2008.

[19] I. Foster, Y. Zhao, I. Raicu and S. Lu, Cloud computing and grid computing 360-degree compared, *Grid Computing Environments Workshop*, IEEE, 1–10, 2008.

[20] A. Bessani, M. Correia, B. Quaresma, F. Andre and P. Sousa, DepSky: dependable and secure storage in a cloud-of-clouds, *ACM Transactions on Storage (TOS)*, ACM, 9, 4, 12, 2013.

[21] M. Alzain, B. Soh and E. Pardede, A new model to ensure security in cloud computing services, *Journal of Service Science Research*, Springer, 4, 1, 49–70, 2012.