Cloud Computing – A Unified Approach for Surveillance Issues

IOP Conf. Series: Materials Science and Engineering **225** (2017) 012073 doi:10.1088/1757-899X/225/1/012073

Cloud Computing – A Unified Approach for Surveillance Issues

Rachana C R[1], Dr. Reshma Banu2, Dr. G F Ali Ahammed3, Dr. Parameshachari B D4

[1]Associate Professor & Head, DoS in Computer Science, Pooja Bhagavat Memorial Mahajana Education Centre, K.R.S. Road, Metagalli, Mysuru-16.
[2]Professor & Head, Department of I S E, GSSSIETW, Mysore, Karnataka, India.
[3]Associate Professor, Department of Computer Science Engineering, VTU Post Graduate Centre, Mysuru.
[4] Professor & Head, TCE Dept., GSSSIETW, Mysore, Karnataka, India.

rachanacr@gmail.com, reshma127banu@gmail.com, aliahammed78@gmail.com, pbdgsss@gmail.com

Abstract- Cloud computing describes highly scalable resources provided as an external service via the Internet on a basis of pay-per-use. From the economic point of view, the main attractiveness of cloud computing is that users only use what they need, and only pay for what they actually use. Resources are available for access from the cloud at any time, and from any location through networks. Cloud computing is gradually replacing the traditional Information Technology Infrastructure. Securing data is one of the leading concerns and biggest issue for cloud computing. Privacy of information is always a crucial pointespecially when an individual's personalinformation or sensitive information is beingstored in the organization. It is indeed true that today; cloud authorization systems are notrobust enough. This paper presents a unified approach for analyzing the various security issues and techniques to overcome the challenges in the cloud environment.

Keywords: Attributes, Cloud computing, deployment models, security, service models.

1. Introduction

Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Computing nodes include end user computers, data centers, and cloud services[14]. Cloud computing advantages include[13]: Lower capital costs, Lower IT operating costs, Absence of hardware or software installation or maintenance, Optimized IT infrastructure. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licenses, the benefits include low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations [2].The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4, 5, 6, 7].Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant

barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters [8]. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels can be achieved and how applications security is moved to Cloud Computing [9]. That uncertainty has consistently led information executives to state that security is their prime concern with Cloud Computing [10].

2. Cloud Attributes

The National Institute of Standards and Technology definition document [PT09] depicts five attributes. These attributes describe a cloud based system as a general model providing metered on demand services to the clients.

The five essential characteristics are as follows[11]:

- **On-demand self-service**. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access**. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity**. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.
- **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The other common characteristics of the cloud include massive scale, service orientation, homogeneity, virtualization, advanced security, low cost service, geographic distribution, and resilient computing.

3. Service Models

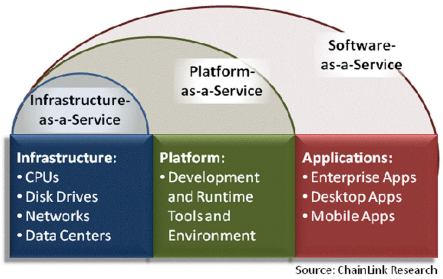

Figure 1: Cloud Service models

Once a cloud is established, the method of its cloud computing services deployment in terms of business models can differ depending on requirements. The primary service models being deployed are: **Software as a Service** (SaaS) — Consumers purchase the ability to access and use an application or service that is hosted in the cloud. The necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud. Examples could include Enterprise Resource Planning, Government apps, e-meetings etc.**Platform as a Service** (PaaS) — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed.**Infrastructure as a Service** (IaaS) — Consumers control and manage the systems in terms of the operating

systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS [10].

4. Deployment of Cloud Services

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. As in figure.2, **A Public cloud's** services are offered over the Internet. It is available to any customer who pays for the service and is owned and operated by the service provider. In a **private cloud**, the cloud infrastructure is operated solely for a specific organization, and the cloud may exist on or off the premises. In a **community cloud**, the service is shared by several organizations that have similar requirements. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

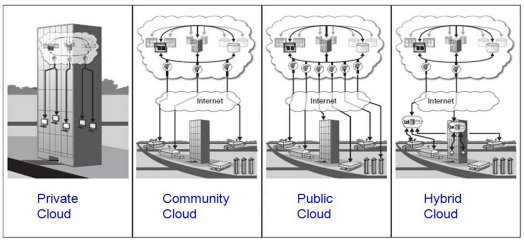

Figure 2: Cloud deployment models

A **hybrid cloud** is usually provided in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms.

Technology faces many challenges today. The robust technologies include Wireless Networks, Wireless devices connected to the network, systems in the cloud, and so on. In order to avoid these threats and to permit authorized use,research efforts have beenundertaken focusing on the followingareas: protocol and network security, data and privacy,identity management, trust and governance, fault tolerance,security, and privacy[19].Cloud computingalso brings with it new security challenges. Although the public cloud model is appropriate for many non-sensitive needs, the fact is that moving sensitive information into any cloud not certified for such processing introduces inappropriate risk [18].Figure. 3 clearly shows security as a major challenge in cloud environments.

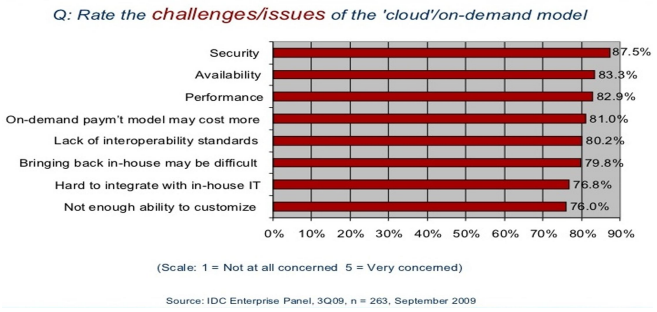

Figure 3: Security: a major challenge, Source: Source: IDC Enterprise Panel, 3Q09, n = 263, September 2009

5. Security Issues in The Cloud

Cloud security concept requires total situational awareness of the threats to the network, infrastructure and information.

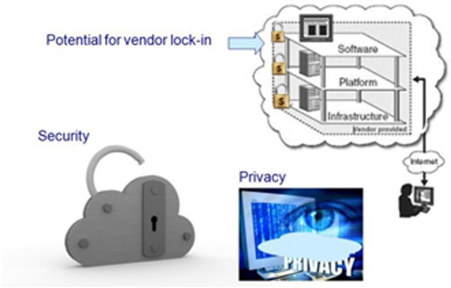

Figure 4: Challenges of Cloud Computing

Data in the cloud typically resides in a shared environment, but the data owner should have full control over who has the right to use the data and what they are allowed to do with it once they gain access. Information security is an area of concern in cloud environment [15]. Figure.4 depicts the challenges which include the issue of vendor lock-in. The vendor lock-in problem is the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move to a different vendor in future without substantial costs, legal constraints, or technical incompatibilities [16].

Table 1: Top three security concerns for cloud services.

1	**Lack of Control over the Location of Data**
2	Increased Vulnerabilities from Shared Infrastructure
3	Privileged User Abuse at the Cloud Provider

Apart from the concerns depicted in Table 1, the following are the most important cloud security threats discussed in [4]:

i. Abuse and nefarious use:
- Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities.
- Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

ii. Insecure interfaces and APIs:
- While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services.
- Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

iii. Malicious insiders:
- The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets.
- Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation.
- As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumer of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

iv. Shared technology issues:
- Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization.
- As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain un-authorized access to data.

v. Data loss or leakage:

- Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust.
- Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

vi. Account or service hijacking:

- Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services.
- Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

vii. Unknown risk profile:

- When adopting a cloud service, the features and functionality may be well advertised, but few questions like - What about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? - How are your data and related logs stored and who has access to them? - What information if any will the vendor disclose in the event of a security incident? Needs to be addressed.
- Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

6. Effective Data Security Techniques

The seven of the specific security issues pointed by Gartner in [3] speaks about the questions/issues the customers must raise with vendors before selecting a cloud vendor: clients must ask the providers to supply specific information on the hiring and oversight of privileged administrators along with the controls over their access, Are their cloud computing providers subjected to external audits and security certifications?, Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, the cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists on data, Ask the provider if they have "the ability to do a complete restoration, and how long it will take?", request for support for specific forms of investigation, and Ask potential providers how the customer can get their data back in case of a disaster?.

The most effective data security techniques for the cloud are [20]:

- **Devising difficult-to-guess passwords**. The most secure passwords incorporate several characteristics to deter hackers, including lower- and upper-case letters, numbers, and special symbols. They should also include 10 or more characters.
- **Providing limited access.** Third-party cloud vendors/Staff should have access only to the data which fall into purview to carry out their jobs.
- **Backing up sensitive files.** Backing up files virtually and physically can happen. Provided, recovery is possible in case of disasters.
- **Implement a strong encryption plan.** From mobile devices to PCs to cloud storage solutions, every place a business stores private data should have the highest level of encryption possible. Passwords, zip files, and encryption software help keep information in the right hands and out of hackers' reach.

Figure 5: Best Practices of Intel for cloud security.

Figure.5introduces the best practices applicable to vendors as well as clients to get over majority of the threats faced in the cloud environment. Further, to ensure security, cryptographic approaches and usage policy rules may be considered. When someone wants to access data, the system should check its policy rules and reveal it only if the policies are satisfied [1]. Sensitive data should be encrypted, both when it is stored on some medium and also when the data is in transit across a network - for example, between storage and processing, or between the provider's system and a customer system. An extra consideration when using cloud services concerns the handling of encryption keys - where are the keys stored and how are they made available to application code that needs to decrypt the data for processing? It is not advisable to store the keys alongside the encrypted data [17].

7. Conclusion

Cloud Computing services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. A number of threats to cloud security exists which include data breaches, Weak identity, credential and access management, Insecure interfaces and APIs, System and application vulnerability, Account hijacking, Malicious insiders, Advanced persistent threats, Data loss, Abuse and nefarious use of cloud services, Denial of service and so on. With respect to privacy, cloud providers must ensure that all critical data (credit card numbers, for example) is masked and that only authorized users have access to data in its entirety. Further, digital identities and credentials must be protected. When it comes to protecting data in the cloud, data and network encryption are considered quite effective. This paper has presented a unified approach towards identifying the major security issues in the cloud environment. An attempt is also made to identify the techniques for effective data security on the cloud.

REFERENCES

1. [1] Hassan Takabi and James B.D. Joshi University of Pittsburgh, Gail-JoonAhn Arizona State University, Security and Privacy Challenges in Cloud Computing, Co-published By The IEEE Computer And Reliability Societies, November/December 2010. http://csis.pace.edu/~marchese/SE765/Paper/security2.pdf https://www.linkedin.com/pulse/20140907071547-305726885-iaas-pass-saas-the-cloud-101
2. Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', Infoworld. http://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html
3. Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0., 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
4. Marinos A, Briscoe G: Community Cloud Computing, 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.
5. Centre for the Protection of National Infrastructure: Information Security Briefing 01/2010 Cloud Computing. 2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

6. Khalid A: Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP'10) 2010, 278–281
7. KPMG: From hype to future: KPMG's 2010 Cloud Computing survey, 2010. Available:http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291
8. Rosado DG, Gómez R, Mellado D, Fernández-Medina E: Security analysis in the migration to cloud environments. Future Internet 2012, 4(2):469–487.
9. Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.; 2009.
10. Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology, NIST Special Publication, 800-145, September 2011.
11. http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085
12. Randy Romes, The Benefits and Risks of Cloud Computing, CliftonLarsenAllen, August 2013. http://www.claconnect.com/resources/articles/the-benefits-and-risks-of-cloud-computing
13. Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, Data Security Issues in Cloud Environment and Solutions', 2014 World Congress on Computing and Communication Technologies, IEEE.
14. http://nbtmv.blogspot.in/2012/01/cloud-computing-from-perspective-of-it.html
15. Michael A, Armando F, Rean G, Anthony DJ, Randy HK, Andrew K, Gunho L, David AP, Ariel R, Ion S, Matei Z (2010) A view of cloud computing. Communication ACM 53(4):50–58
16. Cloud Standards Customer Council Security for Cloud Computing: 10 Steps to Ensure Success, Version 2.0 (2015). http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf
17. [Vic (J.R.) Winkler, Cloud Computing: Cloud Security Concerns, Adapted from "Securing the Cloud" (Syngress, an imprint of Elsevier), November 2011.
18. Dr. ReshmaBanu, Dr. G. F. Ali Ahammed, NasreenFathima, A Review on Biologically Inspired Approaches to Security for Internet of Things (IoT), International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, 978-1-4673-9939-5/16 ©2016 IEEE.
19. Drew Hendricks, 6 Steps to Keeping Your Company Data Secure in the Cloud, http://www.inc.com/drew-hendricks/6-steps-to-keep-your-company-data-secure-in-the-cloud.html

BIOGRAPHY

Dr. ReshmaBanu working as Professor & HOD in the Department of Information Science & Engineering at GSSS Institute of Engineering and Technology for women, Mysuru. She is having 14 years of Teaching and Research Experience. She pursued Ph.D., Computer Science & Technology, from Sri Krishna Devaraya University, Anantapur, Andhra Pradesh. Master of Technology, Computer Science & Engineering, from Visvesvaraya Technological University, Belagavi, Bachelor of Engineering in Computer Science & Engineering, Kuvempu University, Shimoga, Currently Nominated as Coordinator for implementation of ICT initiative's to VTU from GSSSIETW, Mysuru. She is Examiner/valuator/ Paper setter for Visvesvaraya Technological University, Belagavi. She has published several Research papers in International, National Journals/conferences. She is a Member of CSI, IAENG, IBM Academic Initiative, and LM ISTE.Dr.ReshmaBanu's area of interest and research include Networking, Performance enhancement algorithms, Cloud Computing, cryptography and Communication. She has chaired a number of sessions at conferences. She has won the Young Scientist Award from VIRA-2016 for the Initiatives, Discoveries and Developments in the discipline of Wireless Communication Networks. She has received young scientist award from Aufau Internal Awards and Venus International Research Awards.She is theOrganizing Chair for IEEE International Conference- 2016, at GSSSIETW-Mysuru. She is nominated as Special Session Co-ordinator for Elsevier Conference, International Conference on Advanced Material Technologies (ICAMT)-2016 organized by Indo American Institutions - Technical Campus(IAITC), Visakhapatnam, Andhra Pradesh, India. Editorial board Member for International Journal of Engineering and Robot Technology. She is one of the Reviewers for The Fifth International Conference on Cyber Security, Cyber Welfare and Digital Forensic

(CyberSec2017). Four Research Scholars have been awarded Ph.D. Degree under his supervision

Smt. Rachana C R is working as Associate Professor & Head in the Department of Studies in Computer Science, Post- Graduate Wing of SBRR Mahajana First Grade College, K.R.S Road, Metagalli, Mysuru which is affiliated to University of Mysore. She has 13 years of teaching experience in Computer Science. She obtained her B.E in Computer Science and Engineering from Adichunchanagiri Institute of Technology, Chikmagalur and M. Tech in Computer Network Engineering from National Institute of Engineering, Mysuru, affiliated to Visvesvaraya Technological University, Belgaum. She has completed her M.Phil.in Computer Science. She is serving as a reviewer of 'The European Journal of Engineering Education'. She has presented/published several Research papers in International, National Journals/Conferences. She is a Member of Institution of Engineers (India), Computer Society of India, International Association of Engineers (IAENG), International Association of Computer Science and Information Technology (IACSIT). She has delivered number of special lectures in the area of Computer Science and Soft Skills at various institutions. Her areas of interest and research include Cloud Computing Security, Web Programming, Peer-to-Peer computing, Personality Development and Soft skills and Electronic Commerce.

Dr.Parameshachari B D currently working as a Professor and Head of the Department of Telecommunication Engineering at GSSS Institute of Engineering &Technology for Women, Mysuru.Previously, worked as Asst. Professor in the Dept. of ECE at KSIT, Bangalore.Worked as Associate Professor in ECE Dept. at NCERC, Kerala.Worked as a Senior Lecturer in the Department of ECE at JSSATE, **Mauritius (Abroad).** Before that he was Lecturer at KIT, Tiptur for Seven years. He has total Research & Teaching experience of around **14 Years.** He has Obtained B.E degree in ECE and M. Tech degree in Digital communication Engineering from VTU, Belagavi, India and Completed Ph.D in Electronics and Communication Engineering from Jain University. He is the **First Research Scholar** who completed the research work under the faculty of Engineering in Electronics and Communication Engineering from Jain University, Bengaluru. He has published more than **37** papers in *International Journals*/International Conferences. Received young scientist award from Aufau Internal Awards and Venus International Research Awards. He is serving as a reviewer for the various international Journals/conference also as a session chair for various National conferences. Member of various professional bodies such as IE, ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.. He is nominated as Special Session Co-ordinator for Elsevier Conference, International Conference on Advanced Material Technologies (ICAMT)-2016 organized by Indo American Institutions - Technical Campus(IAITC), Visakhapatnam, Andhra Pradesh, India. Three Research Scholars have been awarded Ph.D. Degree under his supervision