CLOUD COMPUTING: A RESEARCH PERSPECTIVE ON THE SECURITY ISSUES

Dr. Reshma Banu[1], Rachana C R[2], Dr. G. F. Ali Ahammed[3], Parameshachari B D[4]
[1]Professor & Head, Department of I S E, GSSSIETW.
[2]Associate Professor & Head, DoS in Computer Science,
Pooja Bhagavat Memorial Mahajana Education Centre.
[3]Associate Professor, Department of Computer Science Engineering,
VTU Post Graduate Centre.
[4]Professor & Head, TCE Dept,, GSSSIETW, Mysore, Karnataka, India.

Abstract
Cloud computing is computing on the internet, whereby shared resources, software, and information are provided to computers and other devices on demand. Further, it is a network of connected devices which are accessible to users allowing flexibility and cost savings due to economies of scale and accessibility. The vast amounts of media now being consumed on mobile devices like smartphones, tablets and computers require larger storage solutions, which now the cloud is providing. Cloud computing is based on a very fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Challenges of cloud computing include loss of governance, Authentication, Isolation failure, Compliance and legal risks, data protection, service unavailability, vendor lock-in and so on. This paper attempts to bring to light the various aspects and security issues of cloud computing.

KEYWORDS: Cloud, Encryption, IaaS, Security.

I. Introduction

Cloud computing allows the user to store, access and share data from internet-connected devices in one central location. Cloud Computing has become a scalable services consumption and delivery platform in the field of Services Computing. The technical foundations of Cloud Computing include Service-Oriented Architecture (SOA) and Virtualizations of hardware and software. The goal of Cloud Computing is to share resources among the cloud service consumers, cloud partners, and cloud vendors in the cloud value chain. The resource sharing at various levels results in various cloud offerings such as infrastructure cloud (e.g. hardware, IT infrastructure management), software cloud (e.g. SaaS focusing on middleware as a service, or traditional CRM as a service), application cloud (e.g. Application as a Service, UML modeling tools as a service, social network as a service), and business cloud (e.g. business process as a service).

According to research firm Gartner, IoT connects remote assets and provides a data stream between the asset and centralized management systems. Those assets can then be integrated into new and existing organizational processes to provide information on status, location, functionality, and so on. Real-time information enables more accurate understanding of status, and it enhances utilization and productivity through optimized usage and more accurate decision support. Business and data analytics give insights into the business requirements data feed from the IoT environment and will help predict the fluctuations of IoT-enriched data and information.

Data breaches, Compromised credentials and broken authentication, Hacked interfaces and

APIs, Exploited system vulnerabilities, Account hijacking, Malicious insiders, permanent data loss are the various threats to data in the cloud. A number of measures are being undertaken by researchers to protect data in the cloud. Security threats to cloud may occur at three stages: Data at rest, in transit and in use.

II. Cloud Service Models

Infrastructure as a Service (IaaS) - In IaaS, generally the service provider offers a Virtual Machine platform and underlying infrastructure with CPU, memory, storage, and networking. Enterprises then deploy their Virtual Machines into this environment. The enterprise retains control of operating systems (OS), storage data, and applications. In the IaaS model, the enterprise does not control the underlying hardware or hypervisor, but retains significant control over security on the VM level.

• Platform as a Service (PaaS) - In PaaS, the enterprise retains control of applications and limited control over application hosting environment configurations. Otherwise, the enterprise relies on the service provider to provide security.

• Software as a Service (SaaS) - In SaaS, the enterprise retains control of only limited user-specific application configuration settings. In SaaS models, the enterprise relies on the service provider to provide security.

III. Cloud Computing Trends

As cloud computing is making its presence felt in the current scenario, the Prerequisites for Cloud Adoption indicate: Rising computer penetration, Improvement in bandwidth availability, Innovations in commodity server market, Improvements in storage technology [2]. Different survey reports shows that user attitude towards cloud computing adoption is increasing [3].

There are several bottlenecks regarding the perspective of cloud among people. According to a survey conducted by Citrix (www.citrix.com), the perception of cloud: what people believe when it comes to cloud computing is as shown in figure.[1]

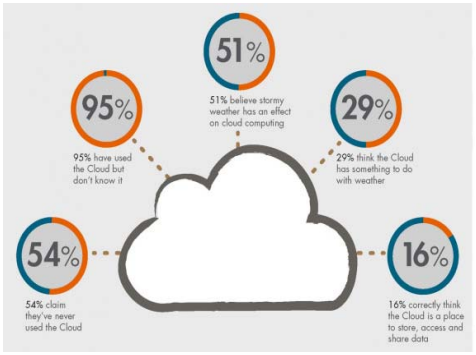

Fig.1: Perception among people about cloud computing

Yet, An increasing move on the part of enterprise businesses to move their information technology services, applications, and infrastructure to a cloud-based architecture will cause market revenue to surge by a factor of three from 2011 to 2017 [5].

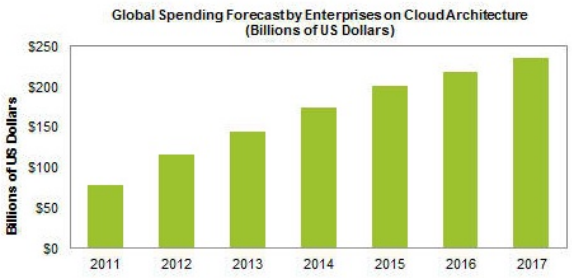

Fig.2: Global Spending Forecast by Enterprises on Cloud Architecture

IV. IoT and Cloud

IoT promises a world of devices and things newly outfitted with Internet that will be able to monitor, communicate and respond when their environments change.

Cloud, is the secret weapon in the Internet of Things. That is because the cloud functions as the equivalent of a big data center offering the system scale that will allow IT to host and store the massive increase in the amount of data heralded by IoT[12].

Key developments in the world of technology further fuelled the propagation and advancement of the Internet of Things (IoT). The major one is cloud computing. Things and devices connected to the Internet, or Internet Connected Devices (ICD) or Smart Devices, generate data on real time that have to be stored, analyzed, secured and used for various purposes. Cloud computing has

paved a way for enabling this at a cost efficient manner[11].

The cloud is destined to be a key component in corporate IoT strategies because of its ability to host vast amounts of data - and enterprises will need every last petabyte. As more companies figure out ways to connect their devices into the IoT networks, which means that all these intelligent refrigerators, washers, dryers, cars and trucks will also be communicating through cloud servers.

Many businesses as shown in figure 3 are evolving their data centers to include virtualization and cloud computing to improve resource utilization, accelerate development and deployment of computer resources, and reduce costs. Despite large investments in data center security appliances, many brands have got compromised.

Fig. 3: IoT and Cloud

V. CLOUD SECURITY ISSUES

New platforms such as a cloud open up additional avenues for threats against data, systems, and reputation. For the most part, these threats are presented through the same types of attacks – data-stealing malware, web threats, spam, phishing, Trojans, worms, viruses, spyware, and more. The information placed on the cloud is often seen as very valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is being placed in the cloud. This makes it critical for the user to understand the security measures that cloud providers has in place, and it is equally important to take personal precautions to secure data placed in the cloud.

As more organizations are placing more workloads in the cloud, the need for expertise has grown. Additional training of IT and development staff will be critical to helping address this challenge[7].

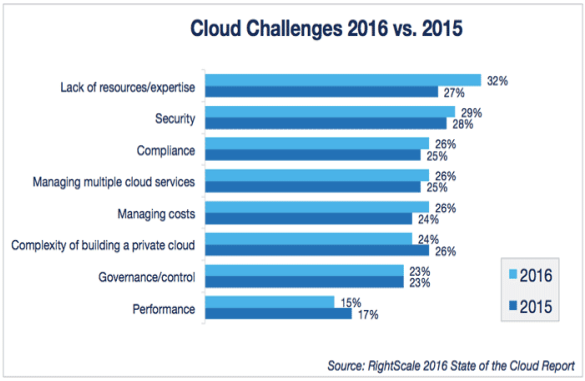

Fig. 4: Cloud Challenges

Once the organization/user decides to move to the cloud, the assets to be moved to the cloud needs to be identified first. Assets could be data/Applications/functions/Process. The most important security/privacy concerns to owners of assets once moved to the cloud include [8]:

– What if the asset becomes widely public & widely distributed?

– An employee of the cloud provider accessed the asset?

– The process of function were manipulated by an outsider?

– The process or function failed to provide expected results?

– The information/data was unexpectedly changed?

– The asset were unavailable for a period of time?

Dynamicity, heterogeneity, elasticity, multi-tenancy all pose security constraints beyond currently available solutions and beyond the concerns of legislation and policy. Two of the more issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers are security and privacy. This slows down the deployment process of Cloud. A particular confidentiality concern in the outsourcing model consists of the fact that the resource host always has full access to the data, even in encrypted cases as the computation requires (local) decryption; as well as lacking control over the location of data with unclear legislation between countries / providers. This demands for enhanced programmability support, but in particular for efficient encrypted computation execution. Whilst security, encryption, authentication etc. have all been concerns of IT for decades now[6]. According to studies in [9], 67% of organizations say managing user identities is more difficult in

the cloud than on-premises One can't risk exposing sensitive company data to unauthorized users. A multi-factor authentication solution can ensure only approved users access the company's cloud-based applications by combining something the user knows, like their ID and password, with something they have, like a token or one-time password delivered to their mobile device.

Software vulnerabilities in cloud software could have a major impact on customers. For example if an Enterprise uses a SaaS email service, which is vulnerable to SQL injection, then this vulnerability could lead to a breach of confidentiality of the customer's emails, severely damaging the Enterprise's reputation. It is important to understand who is responsible for which software component. In the case of SaaS, all the responsibility for preventing software vulnerabilities is with the provider. In IaaS/PaaS, however, the customer is responsible for the software it runs on top of IaaS/PaaS, barring any special arrangements. One complicating factor is that cloud software vulnerabilities become more attractive to attackers/hackers to exploit, because this would allow them to attack many customers at once.

Cloud computing services are consumed and managed via internet connections. This means that customers need to be aware of the risk of network attacks, like spoofing websites, sniffing/eavesdropping network traffic, Denial-of-Service attacks, man-in-the-middle attacks, pharming, wiretapping, etc., on the normal end user interfaces, as well management/administrator interfaces, application programming interfaces (APIs), web services[10].

72% of organizations say the ability to encrypt or tokenize sensitive or confidential data in the cloud is important, and 86% say it will become more important over the next two years[9]. Encryption is a critical last line of defense because it applies protection and access controls directly to the data wherever it resides or as it moves across the company's cloud, hybrid, virtual, and on-premises environments.

Security Guidelines that can be adopted indicate:

1. The cloud user must check with the cloud provider whether effective governance, risk and compliance processes exist.
2. The cloud provider must ensure process that manages people, roles and identities.
3. Privacy policies which are stringent must be enforced in the organization which maintains cloud data.
4. Cloud Networks and connections must be kept secure.
5. Security terms in the cloud service agreements must be managed well.

VI. Conclusion

Virtualization and cloud computing often raise new infrastructure issues that security providers must consider while creating a security foundation to protect against threats. The current effort by security researchers, particularly in encryption, is promising to change the way corporations perceive the security of cloud services. Cloud providers must be asked, Are the services developed using a secure development lifecycle?,What are the data privacy policies?, How is the encryption process carried out on the data in motion and at rest?, What kind of visibility will the user have in the logs? Cloud Computing is here to stay and will contribute to a number of more technological inventions in the years to come.

REFERENCES

[1] Moussa Ouedra ogo, Severine Mignon, HerveCholez, Steven Furnell and Eric Dubois, Security transparency: the next frontier for security research in the cloud, Journal of Cloud Computing Advances, Systems and Applications, DOI: 10.1186/s13677-015-0037-5©, 2015.

[2] "The Cloud Changing the Business Ecosystem," KPMG, 2011.

[3] Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil, Gopakumaran T. Thampi, Cloud Computing – A market Perspective and Research Directions, I.J. Information Technology and Computer Science, 2015, 10, 42-53 Published Online September 2015 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijitcs.2015.10.06

[4] A passion for research, https://softwarestrategiesblog.com/videos-on-the-fundamentals-of-cloud-computing/

[5] GMA News online, Global spending on cloud computing to exceed $320-B by 2017, February 18, 2014 10:18am. http://www.gmanetwork.com/news/story/348922/scitech/technology/global-spending-on-cloud-computing-to-exceed-320-b-by-2017

[6] Lutz Schubert [USTUTT-HLRS] Keith Jeffery [STFC], Advances in Clouds, Research in Future Cloud Computing, Expert Group Report, Public version 1.0, Editors Lutz Schubert [USTUTT-HLRS] Keith Jeffery [STFC]

[7] Cloud Computing Trends: 2016 State of the Cloud Survey, February 09, 2016, Posted by Kim Weins, http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey

[8]Randy Marchany, VA Tech IT Security, Cloud Computing Security Issues, 2010.https://security.vt.edu/content/dam/security_vt_edu/downloads/presentations/cloud_computing.pdf

[9] Ponemon Institute and Gemalto, The 2016 Global Cloud Data Security Study, May 2016.

[10]Dr. M.A.C. Dekker, Dimitra Liveri, European Union Agency for Network and Information Security, Cloud Security Guide for SMEs Cloud computing security risks and opportunities for SMEs April 2015.

[11] Nitin Mishra, Internet of Things (IoT) and the Data Center, September 03, 2014. http://www.netmagicsolutions.com/blog/internet-of-things-and-the-datacenter

[12] Charles Cooper, The IoT, Cloud and Security, CIO, http://www.cio.com/article/2933046/cloud-security/the-iot-cloud-and-security.html

[13] Pradeep Kumar Tiwari, Dr. Bharat Mishra, Cloud Computing Security Issues, Challenges and Solution, International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012)