Survey on Security, Storage, and Networking of Cloud Computing

Mr.Tushar Kailas Mendhe
CT Dept.,ME II nd Year (Wireless Communication & Computing), PCE, Nagpur University
Higna Road, Nagpur-440019(MH), India.
tusharmendhe.2011@gmail.com

Miss.P.A.Kamble,
Asst. Professor, CT Dept. PCE,Nagpur University
Higna Road, Nagpur-440019(MH), India.
pradnya_kamble@rediffmail .com

Mr.Ashish K.Thakre
M Tech. Ist Year, Electronics and Telecommunication Dept., YCCE, Nagpur
Nagpur-440019(MH), India.
ashishthakre.2010@gmail.com

***Abstract*--Cloud architectures constitute cost-efficient moral fibers that will support the transmission, storage, and computing of the applications contents. These infrastructures can be used for scientific and pervasive computing purposes, business. The services delivered through cloud infrastructures increases their exposure to security incidents and attacks. The expenditure and intricacy reduction requirements render the design and development of protection mechanisms.**

Solution features such as authentication, anonymity, survivability, confidentiality, privacy, dependability, and fault tolerance, conflicting. The objective of this is to that modern of security and explores research in protection of cloud communications and networking infrastructures.

A stress will be made on the association of hand held devices in cloud based infrastructures. The essential concepts of cloud computing security will be explored, counting cloud computing security services, cloud computing security principles, cloud security requirements, and testing techniques.

***Keywords*--Cloud security, infrastructure risk analysis, attacks and threats, software and data isolation.**

I.INTRODUCTION

Cloud computing is today’s most inviting technology areas, at least in part, to its cost-efficiency and flexibility. This technology holds the potential to reduce the requirements of expensive computing infrastructure for the IT-based solutions and services that the industry uses. It promises to provide a flexible IT architecture, accessible through internet for hand held devices.

Similarly, open source software enables IT departments to quickly build and set up applications, but at the cost of control and governance. Moreover, virtual machine attacks and Web service vulnerabilities existed. In a cloud computing environment, the entire data inhabit over a set of networked resources, enabling the data to be accessed through virtual machines (VM). Since these data station may lay in any corner of the world afar the get in touch with and control of users, there are diverse security and privacy challenges that need to be understood and must taken care of. Also, no one can refuse the possibility of a server breakdown that has been witnessed. There are various topics that need to be dealt with deference to security and privacy in a cloud computing. In this paper, the fundamental of cloud computing security will be explored, including cloud computing security services, cloud computing security principles, cloud computing security requirements, and testing techniques.

The following items give an overview of the most important topics:

- **Impression on cloud infrastructures**: Cloud infrastructures allow the release of computing, storage, and networking as services rather than products. Three models will be covered in this context:

  (a) Software as a Service (SaaS),

  (b) Platform as a Service (PaaS), and

  (c) Infrastructure as a Service (IaaS).

  The major profit brought by cloud computing, including flexibility and resiliency, cost-effectiveness, data-centric storage, and scalability, will be highlighted.

- **Infrastructure Risk and threat analysis**: To permeate a practical flavor to the attendee, a study of the attacks that have targeted cloud infrastructures will be presented. These attacks have been selected from cases cited by the CSI/FBI crime and security survey and the U.S. Computer Emergency Response Team. Key findings of a recent survey of cloud-computing providers performed by the Ponemon Institute will also be studied. A special emphasis will be placed on the analysis of the vulnerabilities making the number of attacks against cloud computing dramatically increase.

- **Software and data isolation**: A continual threat to a cloud computing environment is that malicious code can interfere with the hypervisor or other virtual machines. An overview of the cloud computing weaknesses such as buffer or out of memory exploits can negotiation the VM, underlying hypervisor and ultimately the host operating system. Sophisticated attacks such as mapping a cloud infrastructure to target a specific service or organization will be given a special interest. The mathematical techniques used in the literature to model the propagation of malicious code, mainly worms, will be covered. The countermeasures that should be implemented to thwart such propagation will be discussed.

II. BASICS OF CLOUD COMPUTING

The cloud computing refers to the development and implementation of models for enabling omnipresent, convenient, on-demand access to a shared set of configurable computing resources (e.g. networks, servers, storage, applications, and services). This encompasses the consideration of network access techniques that guarantee fluid service provider interaction with the cloud users[4]. In the associated business model, users only pay only for the services they actually use, without prior commitment, enabling cost reductions in IT deployment and a scalability of far greater resources, which are abstracted to users in order to appear unlimited, and presented through a simple interface that hides the back-office processes[5]. In the literature, three cloud-based service models have been proposed[6].

1) Software as a Service (SaaS): providing applications running in the cloud, where the customer has virtually no access control or management of the internal infrastructure.

2) Platform as a Service (PaaS): providing a set of tools that support certain technologies of development and the entire necessary environment for deploying applications created by the customer, who is able to control and manage them.

3) Infrastructure as a Service (IaaS): providing basic computing resources such as processing, storage and network bandwidth where the client can run any operating. Below is a list of cloud-based services that have been often cited by researchers and scientist.

- Amazon Web Services (Public Cloud, IaaS): One of the most mature clouds, launched in July 2002 not really with an IaaS offering, more just pieces of it. Its EC2, or Elastic Compute Cloud, which is classified as an IaaS offering launched officially (non-beta) in October 2008.
- Rackspace Cloud Hosting: Launched publicly in February 2008.
- GoGrid (Public Cloud, IaaS): Launched in April 2008.
- Salesforce.com (Public Cloud, SaaS, and PaaS): Although the company was launched March 1999, Salesforces PaaS,
  Force.com was launched in January 2008.
- Google Apps Engine (Public Cloud, PaaS): Its first public beta was launched in April 2008. GovCloud, Googles form of Google Apps that addresses and meets government security mandates was only launched in September 2009.

More recent applications have used the cloud infrastructure for the provision of advanced services such as multimedia streaming[7], virtual reality[8], and robotics[9].

III. RISKS AND THREATS OF CLOUD

The rapid growing of the cloud computing market has motivated malicious users to revise attacks techniques in order to cope with the features of cloud infrastructures.

A. Requirements Security for cloud computing

A set of security requirements for cloud computing have been enumerated:

- **Service and data availability**: Network reliability is a keystone for cloud computing and cloud services. Since a cloud is accessed over public networks, the cloud provider must address the potential for catastrophic loss of Internet backbone connectivity. Availability is also a primary concern for private cloud infrastructures.
- **Confidentiality and privacy:**
- **Disaster recovery and business continuity**: In case of the occurrence of security incidents and disasters Users and application providers should get insurance that the cloud services persist
- **Cloud provider viability**: viability are raised when proprietary interfaces are used to administrate the services accessible to the users.
- **Risk tolerance**: The risk analysis process more challenging since many processes cannot be conducted as in traditional networks. For instance, information classification models should be adapted to handle with

the context where multiple data having different security levels uploaded by users having different access grants should be managed in a single infrastructure.

- **Cost-effectiveness**: One of the key factors used by cloud providers their solutions is that they cost less than whole hardware/software architecture. Also this assumption should not be affected by the security functionalities.
- **Regulation and legislation compliance**: When the data stored or transmitted through the cloud architecture falls under regulatory compliance restrictions, the appropriate deployment (private, public or hybrid) should first be determined. Preventive measures should be implemented to enforce the prohibition of any form of privacy violation. In addition, reactive mechanisms should be used to investigate the cases of privacy violation and take the necessary actions.

B. Attacks against cloud architectures

In the following, a list of the most important attacks that can be conducted against cloud infrastructures is given[11],[12],[13]. Due to space limitations, most of the attacks that are being conducted against information systems and communication networks belong to the Denial of Service (DoS) category. The major novelties regarding these attacks is that coordination is hybrid (i.e., manual and automated) in the sense that public messages are broadcasted to Internet users to participate in the attack process. All what is required is time coordination so that the attack campaign puts down the victim resources. Perfect illustrations of such attacks scenarios are the operations conducted by the Anonymous groups against multiple governmental infrastructures. Other, and more technical, issues regarding these DDoS attacks are polymorphism and evasion. Multiple attacks vectors are sent to the victim infrastructures to enhance the efficiency of the DoS in terms of delay and probability of success. The most common vectors are

HTTP Get flood attack: targeting the web application resources and further modifying the target URL during the attack.

TCP connection flood on port 80: targeting the web application resources.

SYN flood attack: targeting the server TCP/IP stack.

UDP flood attack: targeting network bandwidth resources Evasion techniques are used by the attackers to bypass preventive and reactive security mechanisms. They break into four categories [14]

1) **Packet splitting**: Consists in splitting IP datagram's or TCP streams into non-overlapping fragments or segments. If the security system does not completely reassemble the IP fragments or TCP segments to restore the original application content, it may ignore an attack embedded in the content targeted at the victim host.

2) **Duplicate insertion**: Consists in inserting duplicate or overlapping segments (or IP fragments) to confuse the security system. The efficiency of this technique depends on whether the victim handles the duplicate/ overlapping fragments.

3) **Payload mutation**: Consists in transforming malicious packet payloads into semantically equivalent ones.

4) **Shellcode mutation**: Consists in encoding a shellcodeinto polymorphic forms to evade a protection system that prevents/detects a shellcode according to the signatures extracted from one or a few variants of that shellcode.

Based on the security surveys is that application-level attacks are, by far, more bandwidth-efficient than network-level attacks. This is mainly because, at the application level, attackers often use script injection tools rather flooding tools. This is corroborated by Figure 1.

The most important attacks that can be performed at the application layer include SQL injection and Cross Site Scripting (XSS) attacks, and direct node injection. It is easier to target the application logic or framework of an application than the actual server behind the hardened network perimeter.

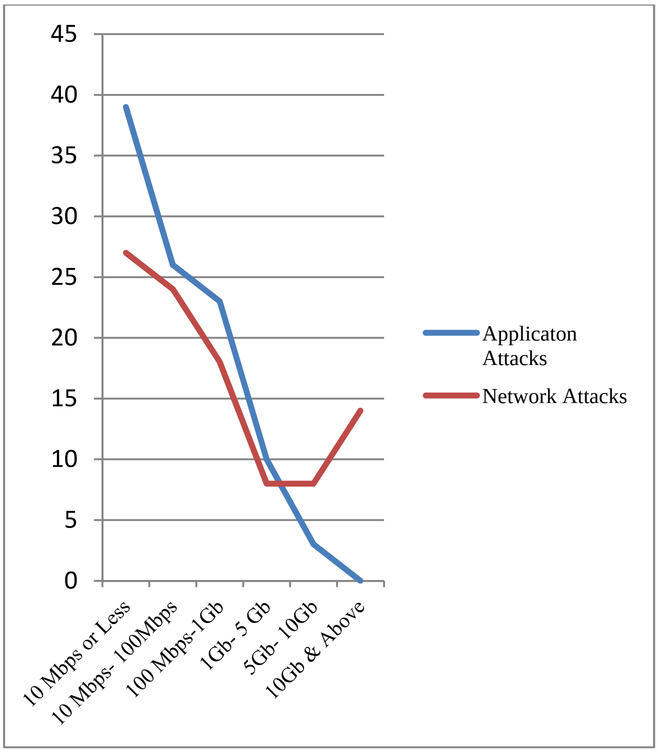

FIGURE: 1

IV.PROTECTION OF CLOUD

A. SaaS protection

A new approach proposed in [15] uses a homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security. This approach supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. Moreover, it is efficient against data modification and server colluding attacks as well as Byzantine failures.

B. Identity management

This scheme in [16] cloud computing use active bundle schemes, where predicates are evaluated over encrypted data and multiparty computing. This presumes that the used encryption schemes allow the execution of predicates without leaving confidentiality and privacy, which is often hard to fulfill. These techniques do not need trusted third party (TTP) for the verification or approval of user identity.

C. Software isolation

To address the security of the hypervisors, different domains are used for providers and users, each with a special trust agent [17]. This encompasses the use of different belief strategies for service providers and customers so as to take time and transaction factors into account for trust assignment. In spite of the efficiency of this approach, its scalability is questionable. Software isolation in a very large scale cross cloud environment is hard to guarantee. This scheme is able to handle only a limited number of security threats in a fairly small environment. In addition, they often have a negative impact on the system performance because of the important computational load.

D. Border Gateway Protocol security

In a Border Gateway Protocol (BGP) [18] architecture has been suggested to detect the cases where an autonomous system may announce itself wrongly as the destination for all the data that is being transferred over that network. This allows the implementation of anomaly detection and incident response mechanisms in cloud computing environments. It also gives us the flexibility to run the secure BGP protocol on some of the autonomous systems in order to protect the wholenetwork. This approach should be accompanied by additional protection techniques since it is itself vulnerable to DoS attacks.

V. CONCLUSION

This provides a conclusion of cloud security techniques, tools, and countermeasures. The security challenges faced by cloud used and providers have been first highlighted. Then, the paper has covered the attacks that can be conducted against cloud-based services. Finally, the countermeasures that are typically used to thwart the aforementioned attacks have been discussed. In spite of the plenty of standards and products dealing with the protection of cloud computing systems, many aspects are still being investigated.

1) **Homomorphic encryption for cloud architectures**: Because the execution of programs is distributed by nature in cloud computing, users cannot be confident where their input and output data is managed. This raises confidentiality and privacy issues that are not fully solved by existing security solutions. An alternative that has been introduced in consists in operating on encrypted functions and encrypted data. This allows addressing the crucial problem of delivering a program that can be executed by a third-party without revealing confidential data. The uses of homomorphic encryption have also been assessed in other contexts where the confidential information is split into multiple pieces that are processed independently by multiple entities [21].

2) **Protection of cloud-based multimedia streaming**: Users are excited to enjoy advantages that networks have provided. The terminals that are used to download and process multimedia streams are short on both the energy and computing resources necessary for the implementation of complex multimedia coding/decoding schemes. Cloud providers may deploy multimedia streaming services to support the provision of monitoring, surveillance, virtual reality, and gaming applications on mobile platforms. New compression techniques have been recently proposed to exploit the abundant resources available in cloud environments in order to allow the implementation of advanced multimedia processing functionalities on resource-impoverished mobile and hand-held terminals (e.g., iPads, smartphones)[22]. Cloud-based secure multimedia coding/decoding algorithms and protocols should focus on the study of: (a) the ability of mobile terminals to delegate the execution of computing intensive decoding algorithms to the cloud infrastructure, (b) the quality of service versus security balance, (c) the impact analysis of terminal mobility on cloud streaming, and (d) the cost-effectiveness of the proposed algorithms and protocols. Progressive multimedia cryptography [23] will be a solid alternative to achieve these objectives.

3) **Digital investigation in cloud computing**: Cloud computing systems base on complex overlaying mechanisms that allow the implementation of flask hardware/software architectures. This poses a challenge to the forensics investigator due to the high volatility of resources such as disk space and memory. Moreover, the distribution of the cloud infrastructure hardens the respect of agreements between users and providers since multiple legislations and regulations should be referred to [24],[25]. Cloud forensics will be among the topics that will be consistently addressed by researchers in the near future.

REFERENCES:

[1] “Security of Cloud Computing, Storage, and Networking” Mohamed Hamdi
School of Communication Engineering, Technopark El Ghazala, 2083 Tunisia, 978-1-4673-1382-7/12/$31.00 ©2012 IEEE

[2] “Security of Cloud Computing Providers Study,” Ponemon Institute, 2011.

[3] V. Winkler, “Securing the Cloud Cloud Computer: Security Techniques and Tactics,” Elsevier Inc., ISBN: 978-1-59749-592-9, 2011.

[4] P. Mell, T. Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145, September 2011 (available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz et al., “A View of Cloud Computing,” Communications of the ACM. Association for Computing Machinery, vol. 53, no. 4, 2010.p. 5058.

[6] B. Sosinky, “Cloud Computing Bible,” Wiley, ISBN: 0470903562, 2011.

[7] Zixia Huang, Chao Mei, Li Erran Li, Thomas Woo, “CloudStream: delivering high-quality streaming videos through a cloud-based SVC proxy,” IEEE Infocom, USA, April, 2011.

[8] Cindy M. Robertson, Blair MacIntyre, Bruce Walker. “An Evaluation of Graphical Context as a Means for Ameliorating the Effects of Registration Error,” IEEE Transactions on Visualization and Computer Graphics, 2009, 15(2), pp.179-192.

[9] Y. Chen, Z. Du, M. Garcia-Acosta, “Robot as a Service in Cloud Computing,” Proceedings of the 2010 Fifth IEEE International Symposium on Service Oriented System Engineering, USA, 2010.

[10] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, Vol. 34(1), pp 111, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.

[11] Computer Security Institute, “Computer Crime and Security Survey,” 2010/2011.

[12] Cloud Security Alliance, ”Top Threats to Cloud Computing,” 2010.

[13] Radware, ”Global Application and Network Security Report,” 2011.

[14] T-H. Cheng, Y-D.Lin, Y-C.Lai, P-C. Lin, “Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems,” IEEE Communications Surveys and Tutorials, Issue 99, pp. 1-10, 2011.

[15] C. Wang, Q. Wang, K. Ren, W. Lou, “Ensuring Data Storage Security in Cloud Computing,” 17th International workshop on Quality of Service, USA, 2009.

[16] Q. Liu, G. Wang, J. Wu, “Efficient Sharing of Secure Cloud Storage Services,” International Conference on Computer and Information Technology, GB, 2010.

[17] S Pal, S. Khatua, N. Chaki, S. Sanyal, “A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security,” Annals of Faculty Engineering Hunedoara International Journal of Engineering, Vol. 10, Issue 1, January 2012.

[18] J. Karlin, S. Forrest, J. Rexford, “Autonomous Security for Autonomous Systems,” Proc. of Complex Computer and Communication Networks, Vol. 52, Issue.15, pp. 2908- 2923, Elsevier, NY, USA, 2008.

[19] M. Brenner, J. Wiebelitz, G. von Voigt, M. Smith, “Secret program execution in the cloud applying homomorphic encryption ,” Digital Ecosystems and Technologies Conference, Korea, 2011.

[20] M. Gomathisankaran, A. Tyag, K. Namuduri, “HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System ,” 45th Annual Conference on Information Sciences and Systems, USA, 2011.

[21] Technology review, Top 10 Emerging Technologies, Massachusetts Institute of Technology. (Available at http://www.technologyreview.com/tr10/).

[22] http://desktop.onlive.com/
[23] M. Hamdi, N. Boudriga, “Chaotic progressive access control for JPEG2000 images repositories”, IEEE Globecom 2008, Computer and Information Network Security Symposium, New Orleans, LA, USA, Nov. 30-Dec. 4, 2008.
[24] S. Zimmerman, D. Glavach, “Cyber Forensics in the Cloud,” IA Newsletter, Volume 14 Number 1, 2011.
[25] K. Ruan, J. Carthy, T. Kechadi, M. Crosbie, “Cloud forensics: An overview,” 7th IFIP International Conference on Digital Forensics, USA, 2011.

Authors Profile:

Mr. Tushar Mendhe received his Graduate Degree in Computer Engineering in 2010 and Pursuing Master’s degree in (WCC) Wireless Communication and Computing from Priyadarshini College of Engg. Nagpur University, Maharashtra, India. He is working as Lecturer in Department of Computer Technology, YCCE College, Nagpur. His areas of interest are Wireless Networks, Distributed Computing.

Miss P. A. Kamble received his Graduate Degree in Computer Science and Engineering in 1992 from Amravati University and Master’s degree in Computer Science and Engineering from Nagpur University, Maharashtra, India. She is working as Asst. Prof. in Department of Computer Technology in Priyadarshini College of Engg, Nagpur. Her areas of interest are VANET. Specializations in field of Network and Database, Ad hoc network protocols.

Mr. Ashish Thakre received his Graduate Degree in Electronics Engineering in 2010 and Pursuing Master’s degree in Electronics and communication from YCCE College, Nagpur University, Maharashtra, India. He is working as Lecturer in Department of Electronics Department, SDMP College, Nagpur. His areas of interest are Wireless Networks, Communication Engg.