Distributed Defense: Enhancing Data Security in Cloud

Laxmi Shankar Awasthi [1], Anand Kumar Rai [2] and Karuna Shankar Awasthi [1*]

[1]Deptt. of Computer Science, Lucknow Public College of Professional Studies, Lucknow.

[2]Deptt. of Computer Science, Mumtaz Post Graduate College, Lucknow.

[*]Corresponding Author: ka7052@gmail.com

ABSTRACT: Cloud computing is a new computer model from grid computing distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and has very useful features such as large-scale calculation and data storage, material performance, high flexibility, high reliability and low cost service. The cloud computing security issue is very important and can prevent the rapid development of cloud computing. This paper has reviewed various software security research papers and introduces a cloud computing system which analyzes cloud computing security issues and their strategies in terms of computer computing concepts and characters. Data privacy and service availability in cloud computing is an important security issue **[1]**. This paper is going to discuss about how to enhance data access security in cloud computing and remove different types of exploitation done by hackers like: Man in the Middle Attack, Dos attack and Cloud Malware Injection Attack.

KEYWORDS: Ddos, Hadoop, Wireshark, Man in the Middle Attack, Packet Sniffing, Glassfish.

INTRODUCTION: Cloud computing is a model that allows for easy network access, which is essential for a shared collection of configurable computer resources (e.g., networks, servers, storage, applications, and services) that can be quickly deployed and deployed with minimal management or service provider interaction **[2].** L. S. Awasthi et al. **[3]** analyzed security issues and threats from cloud computing. To improve software security, the Automatic compiler has been tested that provides a solution for multiple software risks **[4]**. In addition, L. S. Awasthi et al. [**5**] explained about risk assessment and management regarding software security. L. S. Awasthi et al. [**6**] introduced an approach to explain the importance that up to what extent the zombie attack can be vulnerable for the society. L. S. Awasthi et al. [**7**] discussed about software engineering which has positive potential challenges with Crowdsourcing. The Crowdsourcing is a distributed problem-solving methodology in which an undefined number of people participate in an open call to solve a complex problem. A. K. Rai et al. [**8**] have focused on the development of open source software over a limited period of time using specific AI-based project tools. L. S. Awasthi et al. [**9**] have described the role and challenges of gaining more people in management and technology. A. K. Rai et al. [**10**] focused on risk assessment, security and rapid software development. L. S. Awasthi et al. [**11**] reviewed steganography and cryptography in the light of quality software with better security. Gmail is the simple example of cloud computing. There is no need to have software or server with you. If someone has only internet connection, can start sending emails. The server and software for managing email are cloud (internet) and is fully managed by cloud service provider Yahoo, Google etc. and user does not need to do anything. The user gets all benefits of that. 'If someone needs milk, then there is no need to buy cow?' All users or consumers who need to get the benefits of using software or computer hardware such as sending emails etc. Just to get this benefit (milk) they need only internet connection [**12**]. Various Cloud Data Enhancement Studies have been reported.

CLOUD PRIVACY: Privacy is another important concern regarding cloud computing because customer data and business intelligence reside among the cloud servers that can be trusted, managed and maintained by the cloud provider. Therefore, there are potential risks of disclosing personal information like financial data, health records or personal information (e.g., personal profile) to the public or to competitors' businesses. Privacy has become a very important issue [**13**] [**14**] [**15**]. Throughout this document, we consider privacy-maintained as the key attribute of privacy. A few security features directly or indirectly influence privacy protection, which includes confidentiality, integrity, accountability, etc. Obviously, in order to keep private data anonymous, confidentiality is very important, and integrity ensures that data / counts are not corrupted. Cloud Privacy Threats: In a way, privacy is a strong way to maintain confidentiality, in view of the fact that both prevent information leaks. Therefore, if the confidentiality of the cloud is violated, the ability to maintain confidentiality will also be violated. As with other security services, the definition of cloud privacy is twofold: data privacy and computer privacy.

TRUSTED CLOUD COMPUTING OVER DATA CENTERS: Attacks based on malware such as worms, viruses, and DoS exploit system vulnerabilities and give intruders unauthorized access to sensitive information. Unsafe cloud platforms can cause businesses to lose billions of dollars and may even disrupt public services. [**16**]

- **SECURITY-AWARE CLOUD ARCHITECTURE:** We offer a cloud architecture that recognizes the security. This structure helps to block network attacks by establishing trusted operating systems for various cloud applications. Compliance and security require CSPs to protect all data center servers and repositories. Our facilities protect VM monitors (or hypervisors) from software-based attacks and protect data and information from theft, corruption, and natural disasters. It provides robust authentication and authorized access to sensitive data and much-needed services. We have a few goals for designing a reliable and reliable cloud when we create our buildings.
- **VISIBLE NETWORK SECURITY AND MUTUAL TRUST:** Visible network security protects VMs from verified data centers and prevents data loss from some employers. Users must use different certificates to provide trust in all public-key infrastructure (PKI) data centers. Negotiations of trust between the various certification authorities (CA`s) resolve policy conflicts.

- **WORM PREVENTION AND DDoS PROTECTION:** Internet worm prevention and distributed protection against DDoS attacks are required to prevent infrastructure from malware, Trojan, and cyber criminals. This requires us to protect collective ownership in public clouds.
- **REPUTATION SYSTEMS AND DATA CENTERS:** We can build reputable systems using peer-to-peer (P2P) technology or a series of shadow systems between visual data centers and distributed file systems (see Figure 3). In those cases, we can protect the intellectual property of our rights by using the poison of active content to prevent phishing. We will discuss using shadow systems in more detail soon.
- **DATA COLOR:** Our architecture uses data integration in a software file or data object level. This allows us to separate user access and close sensitive information from provider access.
- **PROTECTING VISUAL RESOURCES:** Virtualization improves cloud security. First, VMs add an additional layer of software that can be a single point of failure. That is, virtualization allows us to split or split a single portable machine into multiple VMs (such as server integration), which gives each VM a better security separation and protects each partition from DDoS attacks by other components. Security attacks on one VM are isolated and contained - VM failures are not widespread.
- **LOOSE-COUPLED, STATELESS, FAIL-IN-PLACE COMPUTING [17]:** For many years, web-based applications have continued to be loose-coupled and landless. In a computer cloud, these features are especially important because of the powerful cloud computing environment. App images are not deleted. They are discarded and therefore need to be anonymous. If the virtual machine fails, the application should continue to run interrupted. Integration between application components must be free so that failure of any component does not interfere with the overall performance of the application. The component should be able to "locally fail" with little or no impact on the application .Since the app's components are short-lived, they cannot contain data that should continue beyond any application event. Applications should be made as seamless as possible by pushing the state out of the software, by separating processing and data as much as possible. Strategies for doing this include:
  - ➢ Push the status of the user in the form of cookies or status coded in URLs.
  - ➢ Scroll down the status of the background website.
  - ➢ Keep additional copies of data, a strategy used by Hadoop.
  - ➢ Use network-based persistence, for example Terracotta or Shoal on GlassFish Application server.

THREATS TO CLOUD COMPUTING:

1. NETWORK THREATS

- **DOS ATTACK:** DoS (Service Denial or Attack Denial) overwhelm the server with frequent requests for services.

METHODS:

- ➢ Smurf attack
- ➢ SYN flood

- Teardrop attacks

Distributed DoS attacks result in an interesting trade-off for cloud-based services, without the institutional protection guaranteed by your cloud provider (see Figure 1). [**16**][**18**][**19**][**20**]

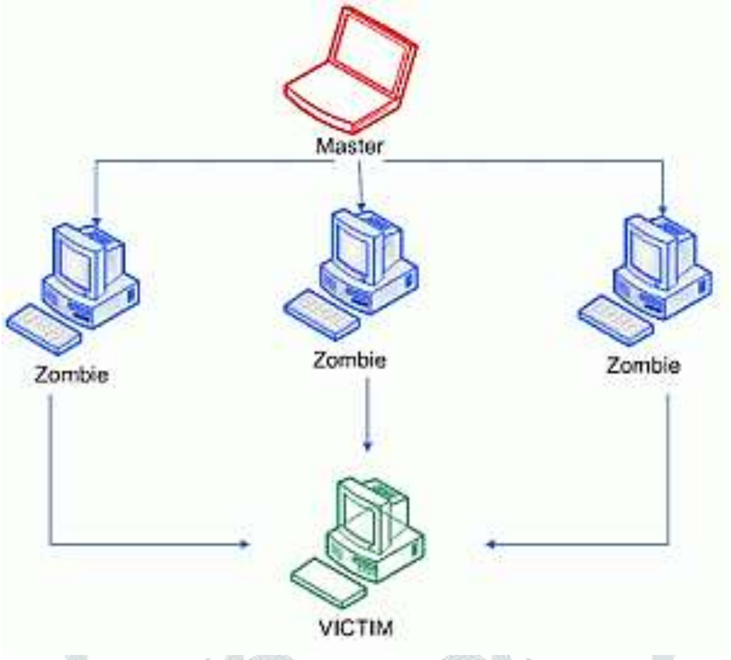

Figure 1

- **MAN IN THE MIDDLE ATTACK:** This attack is carried out when the attacker places himself between two users. Whenever attackers put themselves in contact, there is a chance they can block and modify the communication (see Figure 2). [**21**]

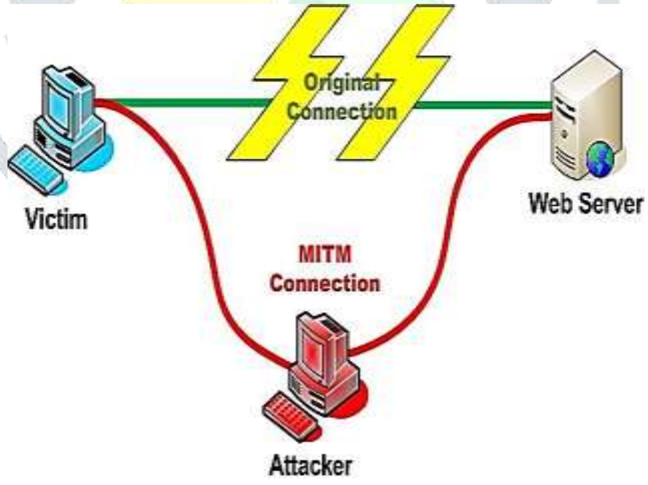

Figure 2

- **PACKET SNIFFING:** Packet odor, network attack strategy, captures network traffic at an independent Ethernet level. After recording, this data can be analyzed and sensitive information can be retrieved. Such a network attack starts with a Wireshark-like tool. Wireshark lets you capture and view data that flows across your network. Any encrypted data is readable, unfortunately, many types of traffic to your network are transmitted as unencrypted data - even passwords and other sensitive data (see Figure 3). [**22**]

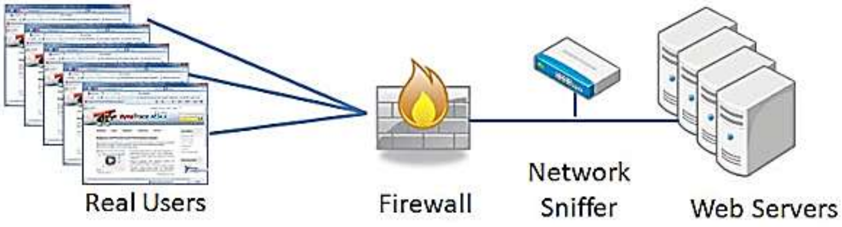

Figure 3

- **XML SIGNATURE ELEMENT WRAPPING (WRAPPER ATTACK):** Wrapping attacks are done by repetition by the user account and password in the login section so that SOAP (Simple Object Access Protocol) messages that is exchanged during the setup phase between the Web browsers and servers are affected by the attackers. [**21**]

2. **SECURITY ISSUES:** Cloud Malware Injection Attack is one of the most widespread attacks. The attack was carried out with a Compromised FTP, and virus actually "sniff out" FTP passwords and return them to the site. The hacker used your FTP password to access your website and added malicious coding I-frames to infect other visitors who were browsing your website. In this attack, enemy attempts are used to inject malicious service or code [**23**] [**24**]. Eavesdropping confirms the success of the attacker on the cloud computer.

PROPOSED MODEL:

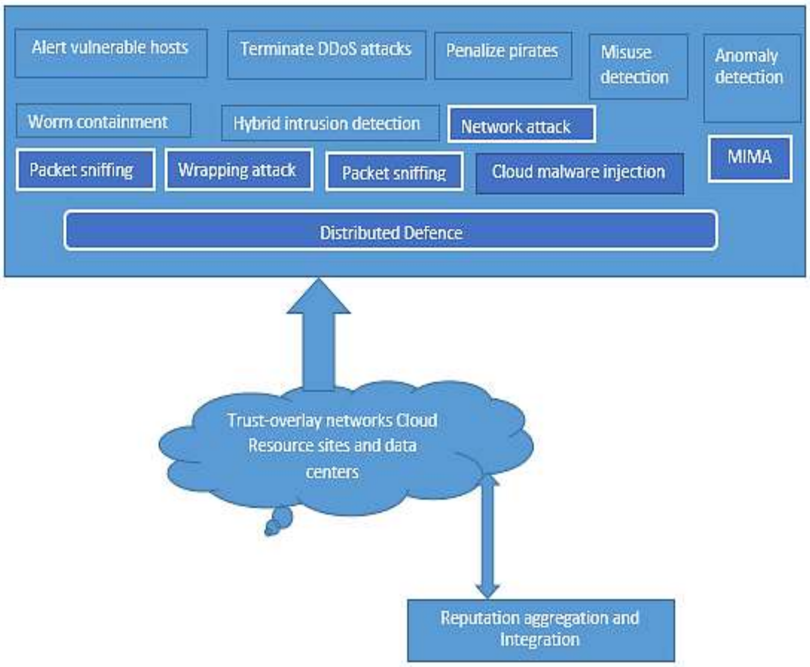

Figure 4

CONCLUSION: We proposed this model of DHT (Distributed Hash Table) figure 4, over cloud resources provisioned from data centers. In the above model, there should be distributed Defense system in the cloud so that various exploitations can be avoided to some extent. Some of the exploitation from which cloud computing can be exploited are: Network attack, Packet Sniffing, Wrapping attack, Cloud malware injection, Man in the Middle Attack. By enhancing the security of distributed defense, we can secure our data in the cloud for unauthorized access, and data leakage.

REFERENCES:

1. http://ieeexplore.ieee.org/xpl/articleDe tails.jsp?reload=true&&arnumber=6202020
2. (Source: NIST Cloud Computing Project*)http://csrc.nist.gov/groups/SNS/cloudcomputing/cloud-def-v14.doc
3. CLOUD COMPUTING: ANALYZING SECURITY ISSUES & NEED OF PREVENTION AGAINST VULNERABILITIES, Laxmi Shankar Awasthi, Himanshu Pathak, Parth Singhal, *International Journal of Soft Computing and Engineering (IJSCE)* , 4, 193-194, 2014.
4. AUTOMATIC COMPILER BASED SECURITY FOR PROGRAM BASED ATTACK IN NETWORKED AND NON NETWORKED COMPUTERS, Laxmi Shankar Awasthi, Anand Kumar Rai and Karuna Shankar Awasthi, ECONSPEAK: A Journal of Advances in Management IT & Social Sciences, 3, 42-55, 2013.
5. REVIEW OF RECENT BREAKTHROUGHS ON THE FOUNDATIONS OF RISK ASSESSMENT AND RISK MANAGEMENT, Laxmi Shankar Awasthi, Santosh Kumar and Karuna Shankar Awasthi, *International Journal of Engineering Research & Management Technology (IJERMT)*, 1, 164-172, 2014.
6. ZOMBIE ATTACK: NEED OF ADVANCE PREVENTION, Laxmi Shankar Awasthi, Himanshu Pathak, and Parth Singhal, *International Journal of Recent Technology and Engineering (IJRTE)*, 3, 34-35, 2014.
7. MOBILE DATA MANAGEMENT USING CROWDSOURCING AS A SERVICE, Laxmi Shankar Awasthi, Santosh Kumar and Karuna Shankar Awasthi, *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE)*, 1, 387-391, 2015.
8. OPEN SOURCE SOFTWARE DEVELOPMENT TIME FRAME MODEL, Anand Kumar Rai, Karuna Shankar Awasthi and Laxmi Shankar Awasthi, *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE)*, 1, 1092-1096, 2015.
9. ROLE AND CHALLENGES OF CROWD SOURCING IN MANAGEMENT AND TECHNOLOGY, Laxmi Shankar Awasthi, Santosh Kumar and Karuna Shankar Awasthi, *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE)*, 2, 4625-4631, 2016.
10. AGILE SOFTWARE QUALITY OF DESIGN RISK ASSESSMENT USING FUZZY LOGIC, Anand Kumar Rai, Karuna Shankar Awasthi, Santosh Kumar and Laxmi Shankar Awasthi, *International Journal of Engineering Research & Management Technology (IJERMT)*, 4, 55-59, 2017.
11. STEGANOGRAPHY AND CRYPTOGRAPHY: A SYSTEMATIC REVIEW, Laxmi Shankar Awasthi, Santosh Kumar and Karuna Shankar Awasthi, *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE)*, 4, 5123-5127, 2018.
12. Security Issues in Cloud Computing , International Journal of Application or Innovation in Engineering & Management (IJAIEM) ,ISSN 2319 – 4847
13. J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,” IEEE Commun. SurveysTuts.DOI:10.1109 /SURV.2011.122111.00145, in press.
14. Y. Xiao, X. Shen, B. Sun, and L. Cai, “Security and Privacy in RFID and Applications in Telemedicine,” IEEE Commun. Mag., Vol. 44. No.4, Apr. 2006, pp. 64-72.
15. H. Chen, Y. Xiao, X. Hong, F. Hu, J. Xie, “A Survey of Anonymity in Wireless Communication Systems,” (Wiley Journal) Security and Communication Networks, Vol. 2 No. 5, Sept. /Oct., 2009, pp. 427-444.
16. Trusted cloud computing with secure resources and data coloring 1080-7801/10/$26 2010 by IEEE.

17. Introduction to cloud computing architecture (white paper 1st edition,June 2009)

18. Above the Clouds: A Berkeley View of Cloud Computing"

19. Survey of network-based defense mechanisms countering the DoS and DDoS problems.

20. OverDoSe: A Generic DDoS Protection Service Using an Overlay Network.

21. Cloud Computing Security Issues with Possible Solutions ISSN: 0976-8491 (Online)

22. Common Network Attack Strategies: Packet Sniffing By Edward Tetzfrom Cisco Networking All-in-One for Dummies.

23. Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu, H. Raghav Rao, ―The Information Assurance Practices of Cloud Computing Vendors‖, IT Pro July/August 2010, InIEEE Computer Society, p. 29-37.

24. Cloud Computing: An Analysis of Its Challenges & Security Issues.ISSN 2277-5420.