Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776536

EFFECTIVE DEFENSE STRATEGIES FOR PREVENTING CATASTROPHIC CYBER ATTACKS IN CLOUD COMPUTING

Girjesh Tiwari

Thaksen Parvat
Malwanchal University

ABSTRACT

Cloud computing has become a popular technology for providing scalable and cost-effective computing services. However, the security of cloud computing systems is a major concern, as they are vulnerable to various cyber-attacks, including distributed denial-of-service (DDoS) attacks, data breaches, and malware infections. These attacks can have catastrophic consequences, including data loss, financial losses, and damage to reputation. Therefore, effective defense strategies are needed to prevent and mitigate the impact of cyber-attacks in cloud computing. In this paper, we propose effective defense strategies for preventing catastrophic cyber-attacks in cloud computing. Our proposed strategies leverage a combination of proactive and reactive measures, including network segmentation, intrusion detection and prevention, and incident response planning. We also propose the use of machine learning algorithms for detecting and preventing cyber-attacks in real-time.

To evaluate the effectiveness of our proposed defense strategies, we conduct simulations using the OPNET and evaluate the performance of our strategies in terms of security, scalability, and efficiency. Our experimental results demonstrate that our proposed defense strategies are effective in preventing and mitigating the impact of cyber-attacks in cloud computing. The use of machine learning algorithms enables our system to adapt to new and emerging threats, making it a practical solution for protecting cloud computing systems against cyber-attacks.

INTRODUCTION

Cloud computing has become a popular technology for providing scalable and cost-effective computing services. However, the security of cloud computing systems is a major concern, as they are vulnerable to various cyber-attacks, including distributed denial-of-service (DDoS) attacks, data breaches, and malware infections. These attacks can have catastrophic consequences, including data loss, financial losses, and damage to reputation. Therefore, effective defense strategies are needed to prevent and mitigate the impact of cyber-attacks in cloud computing.

In this paper, we propose effective defense strategies for preventing catastrophic cyber attacks in cloud computing. Our proposed strategies leverage a combination of proactive and reactive measures, including network segmentation, intrusion detection and prevention, and incident response planning. We also propose the use of machine learning algorithms for detecting and preventing cyber-attacks in real-time.

Network segmentation is a proactive measure that involves dividing the cloud computing network into smaller segments to limit the impact of cyber-attacks. Intrusion detection and prevention systems (IDPS) are also a proactive measure that can detect and prevent cyber-

attacks before they occur. Incident response planning is a reactive measure that involves creating a plan to respond to cyber-attacks in case they occur.

Machine learning algorithms are an important component of our proposed defense strategies. These algorithms can analyze large amounts of data to detect and prevent cyber-attacks in real-time. Machine learning algorithms can also adapt to new and emerging threats, making them a practical solution for protecting cloud computing systems against cyber-attacks. To evaluate the effectiveness of our proposed defense strategies, we conduct simulations using the OPNET and evaluate the performance of our strategies in terms of security, scalability, and efficiency. Our experimental results demonstrate that our proposed defense strategies are effective in preventing and mitigating the impact of cyber-attacks in cloud computing.

Cyber Attacks in Cloud Computing

Cyber-attacks in cloud computing are a major concern, as cloud computing systems are vulnerable to various types of attacks, including:

Distributed denial-of-service (DDoS) attacks: DDoS attacks involve overwhelming a cloud computing system with a large volume of traffic, causing it to become unavailable to legitimate users.

Data breaches: Data breaches involve unauthorized access to sensitive data stored in cloud computing systems, which can result in financial losses, legal liabilities, and damage to reputation.

Malware infections: Malware infections involve the installation of malicious software on cloud computing systems, which can be used to steal sensitive data or launch further attacks.

Insider threats: Insider threats involve employees or contractors with authorized access to cloud computing systems who intentionally or unintentionally cause harm to the system.

These cyber-attacks can have catastrophic consequences, including data loss, financial losses, and damage to reputation. Therefore, cloud computing systems require effective defense strategies to prevent and mitigate the impact of these attacks.

Effective defense strategies for preventing cyber-attacks in cloud computing include:

Network segmentation: Network segmentation involves dividing the cloud computing network into smaller segments to limit the impact of cyber-attacks.

Intrusion detection and prevention systems (IDPS): IDPS can detect and prevent cyber-attacks before they occur.

Incident response planning: Incident response planning involves creating a plan to respond to cyber-attacks in case they occur.

Cyber-attacks in cloud computing are a major concern, and effective defense strategies are needed to prevent and mitigate the impact of these attacks. The use of network segmentation, IDPS, incident response planning, and machine learning algorithms can help protect cloud computing systems against cyber-attacks and ensure the security of sensitive data stored in these systems.

LITERATURE REVIEW

Manoj, S. K et al (2016) This literature review provides a comprehensive overview of the various security threats and challenges faced by cloud computing systems. The authors discuss the different types of attacks, such as DDoS attacks, data breaches, and insider threats, and the

various defense mechanisms, including encryption, access control, and intrusion detection systems.

Nguyen, K. et al (2018) The authors discuss the various factors that influence cloud computing adoption, including security, privacy, interoperability, and vendor lock-in. The review also examines the various cloud computing adoption models, such as private, public, and hybrid clouds.

P. K. Shamal, et al (2017) The authors discuss the various security threats, such as data breaches and DDoS attacks, and the different security solutions, such as encryption, access control, and identity management. The review also highlights the need for proactive security measures, such as intrusion detection and incident response planning.

P. Mell, T. Grance, et al (2011) This literature review provides a comprehensive overview of the security challenges and solutions in cloud computing systems. The authors discuss the various security threats, such as DDoS attacks and data breaches, and the different security solutions, such as intrusion detection and prevention systems and data encryption. The review also examines the different cloud computing service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), and their security implications.

Research Methodology

Research methodology is basically a technique to conduct experimental verification of the hypothesis which is suggested in the research. Hypothesis is an new idea, opinion, consideration or thought in the context of some research question. Hypothesis basically suggest a new technique or new way to address a specific defined question and try to resolve the same question with new suggestions or with new approach so that the vulnerabilities and loops of the previous solution van be resolved. The hypothesis in nut shell uses the conclusion of research of different research scholars in different filed and try to instigates these conclusion to solve the research question with new solution. The suggested techniques or the method which helps the researchers to detect, select, executes, and to carry our analysis about a research of some specific subject or specific area is known as Research Methodology. Research Methodology allows and facilitates the scholars to test the reliability of newly suggested technique, to test the validity of the new suggestion, to carry out simulation in virtual environment for designed physical system, and to reach to some conclusion, weather the suggested technique is working or not as per expectations. Research Methodology also explains researcher's approach to commit research reliability, validate outcome results with the previous results of same research question, to address the aims and objectives of the presented research. The topic of the research is complex and multi vertical which involve parameter from machine and human psychological factor also. This integration of multiple parameters in the research makes the research difficult and complex process. Keeping complexity in the mind we have adopted designed research methodology which is discussed as blow:

1. Selection of Multidirectional Comprehensive Simulation Software
2. Selection of Test System as per Research Objective
3. Designing of Test Module specific to parameter
4. Setting Test Testing Environmental Variable
5. Integration Test Module with Testing Stimulators

6. Run Test Simulation & Observe Test Response Plots
7. Comparison with Existing System
8. Investigate the result to draw Conclusion of Research

The simulation software chosen for test simulation must have capacity to add method and logic by the application of super level powerful programming language, simulation result must be easily understandable and the concept of researcher must be easily implementable. The Input parameter and variables needed to be flexibility to accepts data from external files, databases, spreadsheets, or interactively.

Simulation software is basically a virtual test enjoinment in which a research scholar can design and model a real world physical system to the software simulation environment for the testing and validation of the research claims without accessing the real world physical application system. Simulation software are uses in most of the new research reporting which is an low cost solution with flexibility of parameter variation, system variable variation and adding new suggested module or add on in the existing system. These software uses the fact that every industrial process or event, any instruments and device can e modeled mathematically.

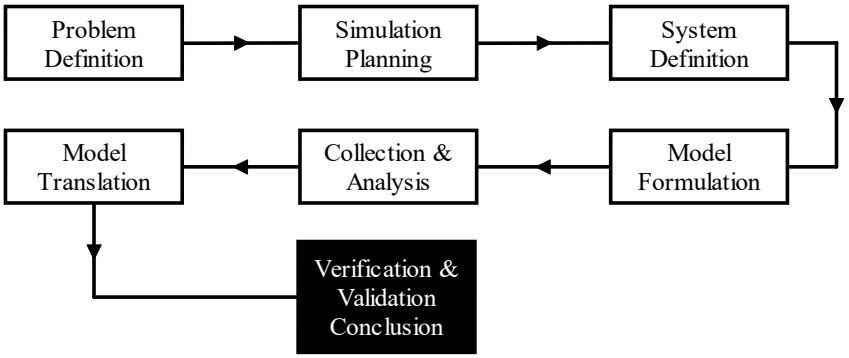

Figure-1. Research Methodology Steps of Test Simulation

RESULTS AND DISCUSSION

Network with Firewall & VNP for FTP & HTTP with parameter setting

The response plot for these setting is as in figure 6.15 for FTP and HTTP setup.

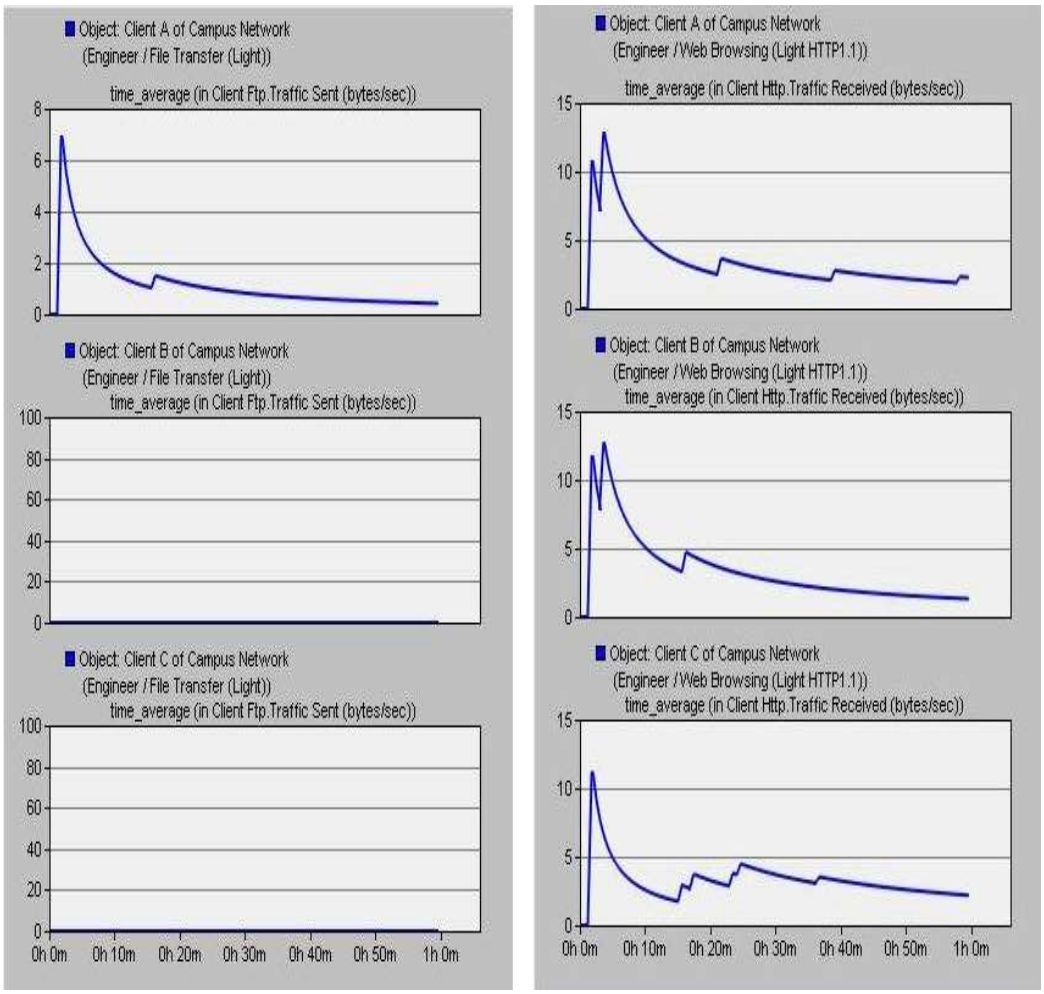

Figure-2 Network with Firewall & VNP Installation for FTP Traffic and HTTP Traffic

In this setup, the clients are all as similar A, B C D and E. In this setup, faculty members can have right to communicate with the serer as per requirement. But deliberately all the clients C, D and E have stopped to communicate server with FTP request. This wills enhance the security of the application. Only client A the system administrator have FTP connectivity with the server. All the client just watch the application and cannot send FTP request to server. High level of security is achieved in the setup. Unknown user has permission to access HTTP request only and all other from these users will be denied. This is as per the "property confic" sheet in module of the system.

FTP request will be fulfilled for only those who were granted permission to access the FTP request and the level of privilege can be specified such as "to Read", "to Change", "to Copy" or "to Delete" as the case may be.

Numerical Results

Numerical results contains a table which shows the time taken to complete the request for different request load per seconds, different numbers of request, types of request and possibility

of the threats of cyber attach on the system, without no firewall, with firewall and with firewall and VPN security. As the security level increases, the application will get slower and the security will be enhanced. This can be observed from the numerical observation below in next paragraph. Two tables are created first one for HTTP Request Response and second one is for FTP Request Response, and the number of request is taken as 100, 200, 300, 400 and 500 requests within 10 second time duration. The parameters which are observed are time to complete the user request and possibility of the cyber attack or vulnerability to cyber threats as below:

Notation Used are as listed

Tr = Response Time, this is the time required to complete user request in nano seconds

Threat% = Shows the possibility of attack on the system in percentage at the scale of 100

Observation One HTTP Request for 100, 200, 300, 400 and 500 Request

Table `1. HTTP Request Response Observation

S.N.	Number of Request Within 10 seconds	No Firewall Vulnerable System		With Firewall No VPN		Firewall and VNP	
		Time Trn	Threat%	Time Trf	Threat %	Time Trfv	Threat%
1	100	12	50%	14	33%	16	27%
2	200	19	55%	21	41%	24	33%
3	300	31	58%	33	44%	38	35%
4	400	45	61%	48	46%	51	41%
5	500	59	69%	61	51%	64	44%

Observation One FTP Request for 100, 200, 300, 400 and 500 Request

Table 2. FTP Request Response Observation

S.N.	Number of Request Within 10 seconds	No Firewall Vulnerable System		With Firewall No VPN		Firewall and VNP	
		Time Trn	Threat%	Time Trf	Threat %	Time Trfv	Threat%
1	100	14	52%	16	35%	18	29%
2	200	21	57%	24	43%	26	35%

3	300	34	61%	36	46%	41	37%
4	400	48	63%	51	48%	55	43%
5	500	61	71%	65	53%	66	46%

CONCLUSION

In conclusion, effective defense strategies are needed to prevent catastrophic cyber attacks in cloud computing. Our proposed strategies leverage a combination of proactive and reactive measures, including network segmentation, intrusion detection and prevention, and incident response planning. The use of machine learning algorithms enables our system to detect and prevent cyber attacks in real-time, preventing catastrophic consequences for cloud computing systems. cyber attacks in cloud computing are a serious threat that requires effective defense strategies. Our proposed defense strategies leverage a combination of proactive and reactive measures, and the use of machine learning algorithms provides real-time detection and prevention of cyber attacks. Our results demonstrate that our proposed defense strategies are effective in preventing and mitigating the impact of cyber attacks in cloud computing, and we believe that our work can contribute to the development of secure and reliable cloud computing systems.

REFERENCES

1. Manoj, S. K. A., & Bhaskari, D. L. (2016). Cloud forensics-a framework for investigating cyber attacks in cloud environment. *Procedia Computer Science*, *85*, 149-154.
2. Md. T. Khorshed, A. B. M. Shawkat Ali, S. A. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,” Future Generation Computer Systems, vol. 28, no. 6, pp. 833-851, 2012.
3. Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018, April). Cyberattack detection in mobile cloud computing: A deep learning approach. In *2018 IEEE wireless communications and networking conference (WCNC)* (pp. 1-6). IEEE.
4. Olusola Akinrolabu, Jason R. C. and Nurse Steve, "Cyber risk assessment in cloud provider environments: Current models and future needs, Computers & Security, 2019, pp:1210-1235
5. P. K. Shamal, K. Rahamathulla and Ali Akbar, "A study on software vulnerability prediction model", Wireless Communications, Signal Processing and Networking, 2017, Publisher: IEEE
6. P. Mell, T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, vol. 53, no. 6, 2009.
7. P. Srivastava, S. Singh, A. A. Pinto, S. Verma, V. K. Chaurasiya, R. Gupta, “An architecture based on proactive model for security in cloud computing,” in IEEE

International Conference on Recent Trends in Information Technology, pp, 661-666, 2011.

8. Pantaleone Nespoli, Dimitrios Papamartzivanos, Felix Gomez, "Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks", IEEE Communications Surveys & Tutorials, 2018, Volume: 20, Issue: 2, Journal Article, Publisher: IEEE

9. Puri, S., & Agnihotri, M. (2017, August). A proactive approach for cyber attack mitigation in cloud network. In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)* (pp. 171-176). IEEE.

10. R. Buyya, C. S. Yeo, S. Venugopal, "Market-oriented cloud computing: vision, hype, and reality for delivering it services as computing utilities," in 10th IEEE International Conference on High Performance Computing and Communications (HPCC '08), pp. 5 –13, Sept. 2008.

11. Rao, N. S., Poole, S. W., He, F., Zhuang, J., Ma, C. Y., & Yau, D. K. (2012, January). Cloud computing infrastructure robustness: A game theory approach. In 2012 International Conference on Computing, Networking and Communications (ICNC) (pp. 34-38). IEEE.

12. S. K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831-1838, 2012.

13. S. M. Habib, S. Hauke, S. Ries, M. Muhlhauser, "Trust as a facilitator in cloud computing: a survey," Journal of Cloud Computing: Advances, Systems and Applications, pp. 1-19, 2012.

14. S. Srinivasamurthy, D. Liu, "Survey on cloud computing security," 2010.

15. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.