ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 4(L), pp. 26365-26367, April, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

IMPLEMENTATION OF A NOVEL PROTECTION SCHEME FOR CLOUD ENVIRONMENT

***Rajashri G. Deshmukh., Vaishali B. Bhagat and Krutika K.Chhajed**

Department of Computer Science, P. R. Pote College of Engineering, Amravati, Maharashtra, India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0904.2045

ARTICLE INFO

Article History:
Received 19th January, 2018
Received in revised form 21st February, 2018
Accepted 05th March, 2018
Published online 28th April, 2018

Key Words:

Cloud Computing, Security, Encryption, IP Grabber, Vulnerabilities.

ABSTRACT

Cloud computing is an innovation methodology for giving pay per utilize access to a gathering of shared resources for specific systems, stockpiling, servers, administration and applications. But with its rapid development the security challenges are numerous. Unsecure practices by cloud service providers (CSP), dependency on web based service delivery and cloud technology related vulnerabilities could lead to application and data compromise. These threat scenarios require cloud customer to look for more transparency and controls. The core component for hosting web applications is the web application server, but to produce secure, reliable, high performance architecture. File manager or file browser is a computer program that provides a user interface to manage files and folders. This system will design cloud based hosting in which file manager will process web content. The web data will be protected by using encryption. The security control used in this system is IP grabber in which it keeps track of IP addresses of all users system. It also provides another technique for scanning a bugs and vulnerabilities in web application.

INTRODUCTION

The Effective Privacy Protection Scheme is proposed to provide the appropriate privacy protection which is satisfying the user demand privacy requirement and maintaining system performance simultaneously. Cloud computing is an emerging computing style which provides dynamic services, scalable and pay-per-use. The different between cloud computing and other computing models are service-driven, sharing resource, and data hosting in outsourcing storage. Sharing resource makes the hardware performance be used more efficient and provides economic benefits for users to reduce the capital cost and additional expenditure. Data hosting in outsourcing storage lets cloud environment rapidly deliver service to users, and do not spend the waiting time of data transmission required by the services. According to the advantages of cloud computing, we can enjoy more convenient services in our daily life [9]. The aim of the proposed system is development of security tool for web application in cloud environment that will help to protect data from malicious insiders. The security tool encryption used for cloud data, IP grabber for checking actual IP of user's system. For scanning bugs in web application, the vulnerability scanner is designed. Along with this, the proposed system aims to maintain data integrity and security, so that lots amount of data can be stored properly without increasing the load of different devices and any type of sensitive information can be stored securely.

MATERIAL AND METHODS

The proposed system consists of peer to peer encryption in which it will encrypt data using private key. This provides string encryption. The web data will be encrypted by using reliable and highly secured algorithm such that data will get secured. The proposed system also includes file manager to perform various operations on a data. It will provide editing tool for user so that data will be manipulated and updated data will be stored on a server. Protection scheme includes an important module, security module that will include various security tools.

Modularized Description

Encryption

A feasible solution for data protection is data encryption. Encryption algorithm offers the benefit of minimum reliance on cloud provider. Encryption is the most effective way to achieve data security. The most widely used symmetric-key cipher is AES, which was created to protect web information. A*dvanced* E*ncryption* S*tandard,* symmetric 128-bitblock data encryption technique will be used to encrypt the data.

Corresponding author:* **Rajashri G. Deshmukh
Department of Computer Science, P. R. Pote College of Engineering, Amravati, Maharashtra, India

IP Grabber

To provide confidentiality of data, admin should know who is accessing their links or data. An IP grabber is a program that will find the IP address of another computer. This will maintain the record of IP addresses that access the web application. It will simply grab IP addresses that access the link that will be notify by system. It will report to the system. All list of IP addresses are kept into log file of grabber.

Vulnerability Scanner

A security tool that will perform scanning operation on website and it will scan bugs and vulnerabilities from the website. So that website will get protected from any malicious code entry. The Open Web Application Security Project (OWASP), an online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of network security. A vulnerability scanner is software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results. However, because both administrators and attackers can use the same tool for fixing or exploiting a system, administrators need to conduct a scan and fix problems before an attacker can do the same scan and exploit any vulnerability found. The vulnerability scanner allows early detection and handling of known security problems. There are main types of vulnerabilities are scanned.

SQL Injection: Injection flaws, such as SQL injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Example Attack Scenarios

Scenario #1: The application uses untrusted data in the construction of the following vulnerable SQL call:

String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";

Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g., Hibernate Query Language (HQL)):

Query HQLQuery = session.create Query("FROM accounts WHERE custID='" + request.getParameter("id") + "'");

In both cases, the attacker modifies the 'id' parameter value in her browser to send: ' or '1'='1. For example:

http://example.com/app/accountView?id=' or '1'='1
This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify data or even invoke stored procedures.

Cross-site Scripting (XSS): XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious activity.

Algorithm Used

Scanning Algorithm

1. Start
2. Enter the URL.
3. Select the type of vulnerability you want to scan for:

- SQL Injection: checks for SQL injection.
- XSS: checks for cross site scripting.

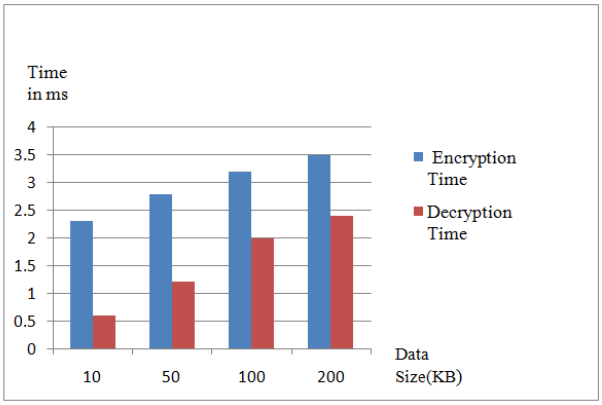
4. Start scanning.
5. After observing the conditions of the selected vulnerability prepare a report

RESULT AND DISCUSSIONS

The step by step workflow of the proposed system and the algorithm that perform its operation is explained in above sections. Now the experimental result shows that a protection scheme using vulnerability scanner gives better prediction result. For encryption we have checked for time required to perform encryption and decryption

Performance of encryption algorithm is evaluated considering the following parameters.

- Encryption Time
- Decryption Time



Graph AES encryption and decryption timing

Graph shows that for the size of 10, 50, 100 KB of data, the encryption timing is 2.3, 2.8, 3.2 milliseconds respectively and the decryption timing is 0.6, 1.2, 2 milliseconds respectively. As the size of image increased the encryption time as well as decryption time increased in AES algorithm.

Table 1 Accuracy of vulnerabilities

Vulnerability Category	Accuracy
SQL injection	93.36%
Denial of service	87.54%
Leakage of data	85.26%
Server Misconfiguration	71.25%
Authorization	72.64%

Now we checked for vulnerability scanner following table 1 shows the prediction accuracy of proposed system. According to vulnerability categories result obtained by proposed system shows in percentage. For all vulnerabilities the system shows the highest percentage to all vulnerabilities defined by OWASP.

Advantages

1. Improves protection to the data and web applications in cloud storage.
2. Provide authentication in open shared network.

3. String encryption is used such that both encryption and scanner are provided at same place.
4. The advantage of vulnerability scanners is to increase network security. High accuracy of detecting vulnerabilities.
5. Less time requires for encryption and vulnerability scanning.

CONCLUSION

In this paper, a novel protection scheme for cloud environment is proposed. This AES and scanner algorithm has excellent performance in generalization so it can produce high accuracy in encryption and scanning of websites. AES encryption provides Stronger and faster than Triple-DES and also provides full specification and design details. Vulnerability scanner will scan vulnerabilities from application that protect web application from insider attacks. A vulnerability scanner allows early detection and handling of known security problems. This result analysis performed evidentially proved that proposed method shows the good performance of security of web application

Acknowledgment

I would first like to thank my guide Prof. Vaishali B. Bhagat of the P. R. Pote College of engineering. My Co-guide Prof. Krutika K. Chhajed was always willing to answer of any query about my research or writing. She consistently allowed this paper to be my own work, but steered me in the right the direction whenever she thought I needed it. I would also like to thank the experts who were involved in the validation survey for this research project. Without their passionate participation and input, the validation survey could not have been successfully conducted.

References

1. Wei-1Fa Liao, Hung-Min Sun, Wei Wu, "A Distributed and Autonomous Guard System Based on Cloud Environments", *IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 2016,*ISBN**:** 978-1-5090-4065-0
2. Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, "Data Security and Privacy in Cloud Computing" In: Hindawi Publishing Corporation *International Journal of Distributed Sensor Networks,* Article ID 190903, 9 pages, http://dx.doi.org/10.1155/2014/190903, Volume 2014
3. MannemSindhuja, PunugotiPavanKumar, "A Trusted Framework for Data Security in Cloud Environment", *In: Journal of network and computer applications,2011,* ISSN: 2319-7064.
4. Nitin Singh Chauhan, AshutoshSaxena." Cryptography and Cloud Security Challenges" *Senior Member IEEE, and JVR Murthy, Infosys Labs, Infosys Limited, Hyderabad, India,2014*
5. Deyan Chen, Hong Zhao."Data Security and Privacy Protection Issues in Cloud Computing". *International Conference on Computer Science and Electronics Engineering, Neusoft Corporation, Shenyang, China, 2012,*ISBN**:** 978-0-7695-4647-6
6. P.Mell and T. Grance. "The nist definition of cloud computing", *National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.*
7. Varun Mahajan, Sateesh K Peddoju."Deployment of Intrusion Detection System in Cloud: A Performance-based Study", *IEEE Trustcom/BigDataSE/ICESS, 2017,* ISSN**:** 2324-9013
8. R. H. Sakr, F. Omara, O. Nomir "An Optimized Technique for Secure Data Over Cloud OS" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May-June 2014 ISSN 2278-6856
9. ZiyuanWang,-Security and privacy issues within the Cloud Computing, International Conference on Computational and Information Sciences, 2011, ISBN: 978-0-7695-4501-1
10. A survey on data breach challenges in cloud computing security: Issues and threat R.Barona,E.A.maryanita2017 international conference on circuit, power and computing technologies, IEEE, ISBN: 978-1-5090-4967-7
11. AkshitaBhandari, Ashutosh Gupta, Debasis das" A framework for data security and storage in Cloud Computing" Computational techniques in information and communication technologies, 2016 international conference , IEEE *https://www.researchgate.net/publication/299338639*
12. U. Greveler, B. Justus, D. Loehr, A Privacy Preserving System for Cloud Computing, ICCIT, IEEE, pp- 648 - 653, 2011.
13. M.Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham, "Towards Privacy Preserving Access Control in the Cloud," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom '11), pp.172-180, 2011.
14. L.A. Dunning, R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", Transaction on Information Forensics and Security, IEEE, Vol. 8, No. 2, pp. 402-413, February, 2013.
15. H. Liu, H. Ning, Q. Xiong, L.T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" Transactions on Parallel and Distributed Systems, Vol. 26, No. 1, pp-241-251, January, 2015.
16. J. Zhou, Z. Cao, X. Dong, X. Lin, "PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems," Journal of selected topics in signal processing, IEEE, Vol. 9 No.7, pp. 1332-1344, October,2015.
17. Y. Wang, "Privacy-Preserving Data Storage in Cloud Using Array BP- XOR Codes," IEEE Transactions on Cloud Computing, Vol. 3, Issue. 4,pp. 425-435, 2015.
18. J. K. Liu, M. H. Au, X. Huang, R. Lu, J. Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services", Transactions on Information Forensics and Security, Vol. 11, No. 3, pp. 484-497, March, 2016

****