International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Detection and prevention of data modification attack based on MD5 algorithm

Miss.Gitanjali A. Kadlag and.Prashant S. Dhotre

Savitribai Phule Pune University, Computer Engineering, DR. D.Y. Patil Institute of Technology, Pimpri, Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Now a day's wireless communication has many issues like Data security and privacy.. Research survey discusses regarding privacy and security is based on the use of internet in traveling, E-Commerce site, social media, banking, study etc. Existing system also often faces the problems with the privacy of the entire network system and stored private data. To avoid these type of issues, increase in widely used application and data complexity, so that web services have design to be a multi-tiered system in that the web server runs the application front-end logic and data is retrieve to a database or file server. Intrusion detection system plays a key role in computer security technique to analysis the data on the server. This problem overcome in proposed Duel Security technique is introduced based on e commerce application. For data security we use the message digest algorithm, an in built web server of windows platform, with database My SQL Server. In this paper proposed system monitoring both web request and database requests. Most of the people do their transaction through web based server use. For that duel security system is used. The duel security system is used to identify & prevent attacks using Intrusion detection system. Duel security prevents attacks and prevents user account data from unauthorized updating from his/her account. Once done all this process then system will more secure for unauthorized data modification attack on database server.

Keywords: *Duel security, MD algorithm, Intrusion detection, multi-tier web application, data leakage detection.*

Introduction

Today database security is a major component of each and every organization. Database is used for the store data in database is not sufficient for any organization, since they have to deal with all issues related to database, from which one of the main issue is database security. In this paper we design with the basic approach that determines whether data stored in database is tampered or not. Any business cannot afford the risk of an unauthorized user observing or changing the data in their databases. Web services are widely used in social network by people. Webservices and applications have become popular and also their complexity has increased. Most of the task such as banking, social networking, and online shopping are done and directly depend on web. Today all are using web services which is present everywhere for personal as well as corporate data they are being attacked easily. Attacker attacks back end server which provides the useful and valuable information thereby diverging front end attack. Data or information leakage is the big issue for companies & institutes. It is very hard for any system administrator to find out the data leaker among the system users. It is creating a serious threat to organizations. It can destroy company's brand and its reputation. Intrusion Detection System examines the attack individually on web server and database server. The multi-tiered web services can be protected by using Intrusion Detection System that is needed to detect attacks by mapping web request and SQL query, there is relationship between request received from the front end web server and those generated for the database back end. Dynamic websites allow persistent backend data modification through the HTTP requests to include the parameters which are variable and depends on the user input. So that the mapping between the web and their database rang from one to many in the mapping model. The MD5 algorithm could be a wide used hash operate manufacturing a 128-bit hash worth. though MD5 was at first designed to be used as a cryptologic hash operate, it's been found to suffer from intensive vulnerabilities. It will still be used as a check to verify information integrity, however solely against unintentional corruption. MD5 was designed by Ronald Rivest in 1991 to exchange associate degree earlier hash operate MD4. In that "MD" stands for "Message Digest."

SQL-injection is a code injection technique that is used to attack data-driven applications, in that SQL queries are inserted into an entry field for execution. The security vulnerabilities in an application software can be exploited using SQL- injection technique, eg. user entered input data is incorrectly filtered for string literal escape characters embedded in SQL statements or user input data is not strongly typed and executed unexpectedly. SQL injection is most commonly known as an attack vector for website applications but that can be used to attack any type of SQL database.

Literature Survey

Muhammad Tayyab, Iqra Ilyas, Aliza Basharat" Solution to Web Services Security and Threats[2018]
In this paper covers the security issues in most popular areas of Health Care Units, e-commerce transactions by comparison of popular algorithms of page rank and trust rank and more security through XML in web services through WS-Security framework by exploring XML signature and its verification and occurrence of major security attacks.[1] Limitation: The problem is that data encryption is done on single column only and can't perform on whole record as making difficult to handle keys.
Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, Chanying Huang." A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users"[2017]
In this paper, author proposes a privacy-aware public auditing technique for shared cloud by using a homomorphic verifiable group signature. the scheme requires at least group managers to recover a trace key cooperatively, that avoid the abuse of single-authority power and provides non-frameability. this scheme also ensures that group users can trace changes in data through designated binary tree; Moreover the security analysis and experimental results indicate that this paper scheme is provably secure and efficient.[2] Limitation: The problem is that, if data not properly divided in block then recover not possible.
Xiaoyong Li , Member, IEEE, Jie Yuan, Member, IEEE, Huadong Ma, Senior Member, IEEE, and Wenbin Yao." Fast and Parallel Trust Computing Scheme Based on Big Data Analysis For Collaboration Cloud Service"[2018]
In this parallel and creative trust computing technique is used that based on big data analysis for the trustworthy cloud service platform environment. First, a distributed and modular perceiving architecture for large-scale virtual machines' service behavior is proposed relying on distributed monitoring agents. Then, an adaptive, lightweight, and parallel trust computing scheme is proposed for big monitored data. To the best of knowledge, this paper is the first to use a blocked and parallel computing mechanism, the speed of trust calculation is greatly accelerated, which makes this trust computing technique suitable for a large-scale cloud computing platform. Performance analysis and experimental results verify feasibility and effectiveness of the proposed scheme.[3] Limitation:(1) Not fast response for a large number of users' service requests becomes a challenging problem.(2)In the process of implementation of the proposed trust computing mechanism, the problem of trust value updating must be considered.
X. Chen, J. Li, X. Huang, J. Ma, and W. Lou. "New Publicly Verifiable Databases with Efficient Updates"[2015]
In that a model is developed which notion of verifiable database (VDB). By using VDB resource-constrained client can securely outsource a large database application to an untrusted server so that it could later retrieve a database record and update it by assigning a new value. Also, any attempt by the server to tamper with the data will be detected by the client. Author proposes a new VDB framework from vector commitment based on the idea of commitment binding. The construction is public verifiable and secure under the FAU attack. Furthermore, he proves that our construction can achieve the desired security properties.[4] Limitation: Necessary authentication process is missing between the auditor & cloud in most existing public auditing schemes.

Proposed Methodology

Our aim to enable strong data detection and protection for web applications while at thesame time we minimize the false positive rate. Our objective to secure three tier web applications for detecting and preventing different types of attacks. Detecting the tempering attack for database activity. Provide both side security front-end and back- end.

A. Architecture

Below fig 1. Show the system architecture including the different module explains in below. Existing application systems are providing one way security for the web applications protecting a web application in terms of interface and at database end with proper recovering options is best part of the system. Proposed system designs new model to provide the security of the ecommerce web applications along with its database in every step.

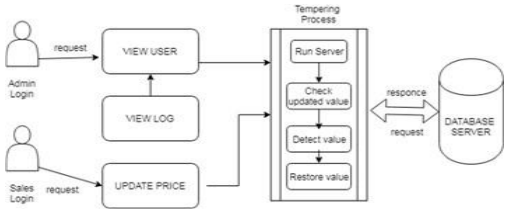

Fig 1. System architecture

Algorithms

Algorithm: Message Digest 5(MD5)

Input: Input data D = D1, D2, D3,.., Dn saves into the hash table.

Step 1: Arrange all input data into matrix format (save into log files).

Step 2: Consider m as a selected data act as a new selected data.

Step 3: m position gets changed after allocated time period.

Step 4: If () data get hacked. Step 5: Data leakage is occurs.
Step 6: We have to check the leakage data and prevent

Step 7: Using Revert back function we have to get original data.

Step 8: When user calls that corrupted file, hash function gives to user a previous data.

Step 9: Return True.

Mathematical Model:

System Description:
Input:

Function DATABASE INTRUSION DETECTION ()
Set V:
V0=Get the time in seconds (T)
V1=Visit Database table for reach interval of T V2=Get a record from the database
V3=Hash it using MD5 Algorithm V4=Create vector of hash values V5=Send to Notarize

Output:
VALIDATOR: (Here this module is responsible for periodically scans the audited
tables, computing the hash values on a per transaction basis.)
Success Conditions: Success system when do not change any value from database.
Failure Conditions: Our system fails when attacker get success form data base insertion.
Comparison algorithm with existing

Parameter	SHA	MD5
Process Speed	Slow	Fast
Bits	160	128
Structure	Complex	Simple
Security	High	High

Software Requirement

Specification
The proposed system created based on the java programing language. Net bean tool used for programing the proposed system. User data is stored in mysql database. This system is used widely accessibly a web technology application using JSP with local server. Web application that facility to access the any data, communicates to each other using the with local server and Trustee Server using REST API.

Result and Discussions

In existing system the protection is the front end and for files, but sometimes the attacker is attacks on the backed also mean database, then that system not protected. Then we work on MD5 Algorithm recommended that the tamper detection complete only for the tiles but in our approach we perform the tamper detection on live data. In our approach This Algorithm gives a systematic path to the employee and auditor for the secure communication with the system. By using this algorithm we stop the database disturbance form insider's and the outsider's. Because of the audit log it is capably auditing the central database.

Table 1 Result

Sr no	Table Name	Product Id	Data & Time
1	Product Details	ID 1	15/01/2020,01:23 PM
2	Product Details	ID 2	16/01/2020,03:45 PM
3	User Details	User Name	17/01/2020,04:00 PM

In this paper we have identified the threats of SQL injection and DOS attack using Intrusion Detection System. Additional security measures can be provided using stored procedures. This approach applies mapping model to detect SQL injection and DOS attacks. Also we have identified the tempering attack on database using MD5 Algorithm. We have achieved this by isolating the flow of information from each web server session with a virtualization technique. We attempted to model static and dynamic web requests with the back-end file system and database queries and also quantified the detection accuracy of our approach.

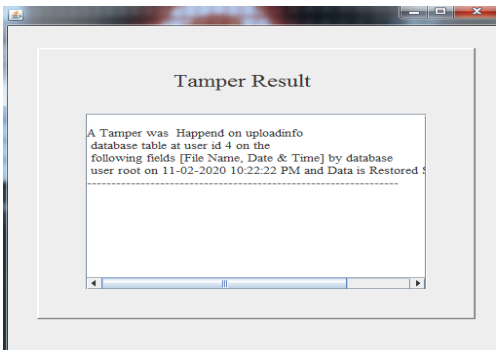

Fig 2. Forensic analysis result

Conclusions

This is an Application of Modified data detection system through unauthorized access. By using MD5 algorithm we are restoring modified data in cooperation the front-end web (HTTP) requests and back end DB (SQL) queries. In future we can analyze the phishing attack and cross site scripting attack can be installed on wide range of machines having different operating systems and platforms. In future we work on global server to analysis the temper server.

Acknowledgment

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well- wishers who supported us in completing this paper successfully I am heartily thankful to my project guide Dr. Prashant Dhotre sir for his valuable guidance and inspiration. In spite of their busy schedules they devoted their self and took keen and personal interest in giving us constant encouragement and timely suggestion. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

References

[1]. Muhammad Tayyab, Iqra Ilyas, Aliza Basharat" Solution to Web Services Security and Threats"2018.

[2]. Anmin Fu, Shui Yu, Yuqing Zhang, HuaqunWang, Chanying Huang." A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users"2017.

[3]. Xiaoyong Li , Member, IEEE, Jie Yuan, Member, IEEE, Huadong Ma, Senior Member, IEEE, and Wenbin Yao." Fast and Parallel Trust Computing Scheme Based on Big Data Analysis For Collaboration Cloud Service"2018.

[4]. X. Chen, J. Li, X. Huang, J. Ma, and W. Lou,New Publicly Verifiable Databases with Efficient Updates, IEEE Transactions on Dependable and Secure Computing, In press, 2015.

[5]. V. Vu, S. Setty, A.J. Blumberg, and M. Walfish,A hybrid architecturefor interactive verifiable computation, IEEE Symposium on Securityand Privacy (SP), pp.223-237, IEEE, 2013.

[6]. S. Pearson and A. Benameur. "Privacy, security, and trust issues arising from cloud computing." Proc. Cloud Computing and Science, pp. 693–702, 2010.

[7]. NIST. "Top 10 cloud security concerns (Working list)."http://collaborate.nist.gov/twiki- cloud computing/bin/view/Cloud Computing. Accessed February 2017.

[8]. M. O'Neill. "SaaS, PaaS, and IaaS: a security checklist for cloud models." http://www.csoonline.com /article/660065/saaspaas-and-iaas-a-security-checklist-for-cloud- models. Accessed August, 2015.

[9]. S. Garfinkel and M. Rosenblum. "When virtual is harder than real: security challenges in virtual machines based computing environments." Proc. 10th Conf. Hot Topics in Operating Systems, pp. 20–25, 2005.

[10]. S. T. King, P. M. Chen, Y-M Wang, C. Verbowski, H. J. Wang, and J. R. Lorch. "SubVirt: Implementing malware with virtual machines." Proc. IEEE Symp. Security and Privacy, pp. 314 – 327, 2006.

[11]. M. Price. "The paradox of security in virtual environments." Computer, 41(11):22–28, 2008.

[12]. J. Luna, N. Suri, M. Iorga andA. Karmel. "Leveraging the potential of cloud security service level agreements through standards." IEEE Cloud Computing, 2(3):32–40, 2015

[13]. P. Mell. "What is special about cloud security?" IT-Professional, 14(4):6–8,2012. http://doi. ieeecomputersociety.org/10.1109/MITP.2012.84.Accesed August 2015.

[14]. S. Pearson and A. Benameur. "Privacy, security, and trust issues arising from cloud computing." Proc. Cloud Computing and Science, pp. 693–702, 2010.

[15]. D. C. Marinescu, Cloud Computing; Theory and Practice, 2nd Ed. Morgan Kaufmann, San Francisco, Ca., 2017.