ISSN 2395-1621

Detection and Prevention of Data Modification Tempering Attack.

[#1]Vivek Kumar Gupta, [#2]Jayant Bonde, [#3]Akshay Gorad, [#4]Priya joshi,
[#5]Professor. V. R. Manga.

[1]guptavivek061997@gmail.com,
[2]jaybonde9923@gmail.com,
[3]akshaygorad4@gmail.com,
[4]priyajoshi301997@gmail.com

[#12345]Department of Computer Engineering

SKN Sinhgad Institute of Technology & Science Lonavala.

ABSTRACT

Now today's entire world have we many issues in internet security and privacy. Research survey discusses regarding privacy and security is based on the use of internet in travelling, 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 overcome these issues, increase widely used application and data complexity, so web services have design to a multi-tiered system wherein 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 ecommerce 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 purpose 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.

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

ARTICLE INFO

Article History

Received: 7th December 2019

Received in revised form :

7th December 2019

Accepted: 9th December 2019

Published online :

9th December 2019

I. INTRODUCTION

Now day's 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. Web services 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. As we are using web services which is present everywhere for personal as well as corporate data they are being attacked easily. Attacker attacks backend server which provides the useful and valuable information thereby diverging front end attack. Data leakage is the big issue for industries & different 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. In order to protect multi-tiered web services an efficient system call Intrusion Detection System is needed to detect attacks by mapping web request and SQL query, there is direct causal relationship between request received from the front end web server and those generated for the database backend. Dynamic web site allow persistent back end data modification through the HTTP requests to include the parameters that are variable and depend on the user input. Because of which the mapping between the web and the database rang from one to many as shown in the mapping model.

The **MD5 Algorithm** is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.

MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4. The abbreviation "MD" stands for "Message Digest.

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

To create a system for intrusion detection on static and dynamic web pages (creating session ID's for each user containing the web front end[HTTP] and back end[SQL server]) also make it able to prevent those intrusions from attacking the web pages and it should be able to find out the perpetrator.

II. LITERATURE SURVEY

X. Chen, J. Li, X. Huang, J. Ma, and W. Lou," New Publicly Verifiable Databases with Efficient Updates", 2015, in this paper author has developed a model which notion of verifiable database (VDB) enables a resource-constrained client to securely outsource a very large database 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 not only public verifiable but also secure under the FAU attack. Furthermore, he proves that our construction can achieve the desired security properties.

Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, Chanying Huang, "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users", 2016, this paper author design a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least group managers to recover a trace key cooperatively, which eliminates the abuse of single-authority power and provides non-frameability. Moreover, our scheme ensures that group users can trace data changes through designated binary tree; and can recover the latest correct data block when the current data block is damaged. In addition, the formal security analysis and experimental results indicate that our scheme is provably secure and efficient.

Ekta Naik, Ramesh Kagalkar, "Detecting and Preventing Intrusions In Multi-tier Web Applications", 2014, In this paper, author proposes implemented double guard using internet information and service manager Furthermore, it quantify the limitations of any multitier IDS in terms of training sessions and functionality coverage. I am implementing the prevention techniques for attacks. I am also finding IP Address of intruder. A network Intrusion Detection System can be classified into two types: anomaly detection and misuse detection. Anomaly detection first requires the IDS to define and characterized the correct and acceptable static form and dynamic behaviour of the system, which can then be used to detect abnormal changes or anomalous behaviour.

V. Vu, S. Setty, A.J. Blumberg, and M. Walfish, "A hybrid architecturefor interactive verifiable computation", 2013, this work is promising but suffers from one of two problems: either it relies on expensive cryptography, or else it applies to a restricted class of computations. Worse, it is not always clear which protocol will perform better for a given problem. He describe a system that (a) extends optimized refinements of the non-cryptographic protocols to a much broader class of computations, (b) uses static analysis to fail over to the cryptographic ones when the non-cryptographic ones would be more expensive, and (c) incorporates this core into a built system that includes a compiler for a high-level language, a distributed server, and GPU acceleration. Experimental results indicate that our system performs better and applies more widely than the best in the literature.

III. PROPOSED SYSTEM

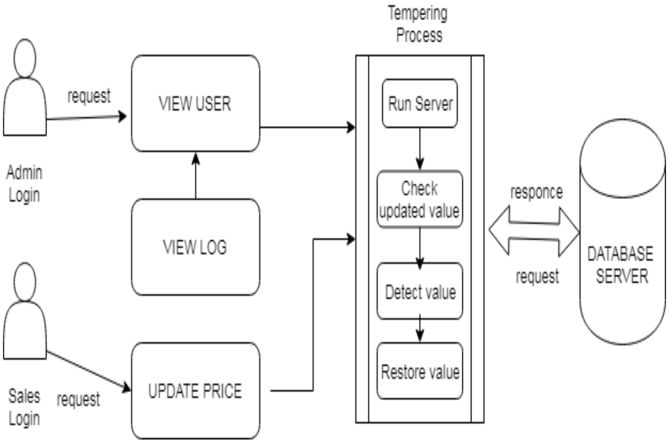

Fig 1. System architecture

Above 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.

Module Explanation:
User Module:
User can authorize login access. He can update all personal information. He also can give authority to generated secure encryption process.

Sales Department:
Sales department work as a hacker. Here hacker changes the database value of any product without authentication.

Admin Module:
Admin is the authorized person, he check all the user activity records as well as profile. He also watch the tempering on changing the values from data base.
Advantages:
1. The proposed system provides authentication.
2. It also prevents hacking.
4. The system prevents identity theft.

Summary: First of all normally database engines are started and tampering detection is initialized as soon as attack is performed a pop up value is generated at the admin's panel and the data value is restored successfully.

IV. 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.

V. CONCLUSION

We propose a tampering detection system, based on data analysis on cloud server. This system is analysis the data modification from unauthorised access. This system design new algorithm form detection and prevention data from cloud server.

REFERENCE

[1]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.

[2] Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, Chanying Huang, "A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" IEEE, 2016.

[3] Ekta Naik, Ramesh Kagalkar, "Detecting and Preventing Intrusions In Multi-tier Web Applications", International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014.

[4] 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.

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