IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. III (Sep.- Oct. 2017), PP 61-64
www.iosrjournals.org

Review Paper on Web Service Security and Logging

[*]Ms.Mehdi Tanweer Mehmooda, Prof. Nagaraju Bogiri
Department of Computer Science K.J College of Engineering & Management Research Pune, India
Department of Computer Science K.J College of Engineering & Management Research Pune, India
Corresponding Author: Ms.Mehdi Tanweer Mehmooda

***Abstract*: "**Web service" is an application running on Internet by a service provider, which is accessible by the users through standard internet protocols. Web Service Security has become significantly important and very harder to achieve which deals with management of authentication, authorization, monitoring and logging of the web services data usage. Web services provides reusability, virtualization, integrity, availability and interoperability through the application of technology such as SOAP and service oriented architecture and Representational State Transfer. Whenever a request is goes to application then the application handles the request and also application engine automatically logs the request. Logs provide lots of valuable and important information about systems, networks, and applications. Logs encompassing audit records, and alerts also provides signs of something is already broken or will be broken in future. Logs also reveal and exposes information that might affect supervisory compliance and even commercial governance. Audit log adds another layer of security into web services through the monitoring. Logs are one of the most effective forms of tracking information for each request made to server and the response return from the server. This paper provides an overview of web service and web service security through monitoring and logging.

Keywords: Web service, Web services security, web-content mining, web structure mining, web usage, web logs.

Date of Submission: 16-09-2017 Date of acceptance: 07-10-2017

I. Introduction

Web Service suppliers and consumer are highly concern about the security and they are adopting evolving standards in security trends. Business should select the emerging trends based upon the business requirements instead of handling all types of security threats. A business should combine different security standards in order to provide complete security to web services. A business can secure web services at transport layer through SSL and at message level through authentication, authorization, message encryption in XML format and XML signature. Web services provides reusability, virtualization, and interoperability through the application of technology such as SOAP, service oriented architecture and Representational State Transfer (REST) [1]. Interoperability is premier and principal for companies that performs the business transactions across multiple boards. Most of the Web services implementations has many challenges to be more precise, they don't always enable security and alert by default, and often leave security decisions about authentication, authorization and audit logging which can cause serious problems. Monitoring and Logging is mandatory in various industries such as Health-Care where audit logging and monitoring controls the systems which has patient data similarly Payment Card Industry Data Security Standard (PCIDSS) has mentions logging as mandatory to monitor and track access to system, network resources and cardholder data [1].

Web services evolve, become even more important for organizations and businesses of all sizes, taking control of Web services monitoring and logging has increased accountability, security and regulatory standard satisfactions.

Web services security has two parts: (i) Interface implementation security (ii) message security. Interface implementation security can be gained by using Web application security controls such as Secure Sockets Layer (SSL).Message security can be achieved by using XML, SAML (Security Assertion Markup Language), XML Signature and XML Encryption. Hence based on the implementation challenges of web services security, it is very important to do monitoring-logging and Data Mining on Web Service usage. In this paper we have explore, reviewed and proposed design to capture web service usage logs in distributed environment and it applies Apriori algorithm to mine associated service usage logs.

II. Web Services

The "Web service" is an application running on Internet by a service provider, which is accessible by the users through standard internet protocols. The World Wide Web Consortium defines a Web service as

1. An application which is identified by a URI
2. It has interfaces and binding

3. The definition of web-service can be discovered by other Web services running on the internet.
4. It can interacts with other Web services through XML language and by using standard protocols.
5. It communicates and exchanges message between the different Web services through SOAP, UDDI and WSDL.

An interesting challenge is handling monitoring and logging in distributed environments such as those of Web services. Unlike operating system logs which are physically located on a single machine or a single network device, Web services are distributed across multiple systems, different technologies and different policies, and even different organizational domains. This creates many constraints on log design in terms of both scope and strength [1].

III. Web Services Security

Web services security includes various layers, as per review web services are loosely coupled in nature and has open access through HTTP protocol hence it is required to enable security at all the layers [4]

- Security at Transport Layer — A web Service can be secured at transport layer by applying firewalls, virtual private networks, secure socket layer etc.
- Security at Message Layer — A web Service can be secured at Message layer by using authentication tokens for verifying requester's identity and authorization to control access.
- Security at Data Layer — A web Service can be secured at Data layer by applying security such as message-encryption and message-digital-signature to protect against data tampering and alteration.
- Security at Web Service Environment — A web Service environment can be secured by applying security such as monitoring-logging, and auditing to track access to system, network resources and application usage.

IV. Literature Review

The overview of amazon web services AWS provides the various security standards that have been used for making web services more secure over the cloud and also applied audit logging to provide complete security [4]. The various existing systems that uses logging mechanisms are

A. Server-side AR System logs implemented by bmc [9]

The server side AR System helps to enables all important logs to capture synchronized activity and provides wide logging capabilities [9], few of the log files are revealed are.

- Error logs — which contains critical state information about the running server, includes errors encountered and timestamps of when the server started.
- API logs — which contains information about each API call made to the server.
- SQL logs — which contains information about each SQL call made by the server to the database.
- Filter logs and Escalation logs — It contains information about the execution of the workflow objects on the server.

B. IBM QRadar Log Manager [11]

IBM QRADAR log Manager which captures and processes event data from thousands of sources and also provide visibility to developing threats and helps to meet continuous monitoring requirements [11].

- It is Scaled to support millions of events per
- Second within a single unified database in real time.

C. Audit Logging in HealthCare

In HealthCare system monitoring and logging is very essential and the process of information disclosure and auditing should imitate the Privacy Act of 1974[13].

The electronic medical records contains more valuable information than the bank account passwords or credit card numbers. This is quite surprising, but the data in the electronic medical records has complete detail information such as

- Patient's names
- Patient's dates of birth
- Patient's addresses
- Patient's phone numbers;
- Patient's places of work and positions
- Patient's IDs, card numbers
- Patient's medical and social insurance.

Patient's electronic medical records can be used for complete identity theft. In our survey of Healthcare system we have evaluated the various business critical operations which has access to patient data and they are

- Update operation
- Access operation
- Search operation
- Delete operation
- Printing operation
- Downloading operation

V. Proposed System

The proposed Frame work design consists of two parts

D. Web Service Logging

In this paper, we have propose a logging mechanism to handle logging in distributed environments such as those of Web services. The client logins to the system with his/her user-ID and performs the transaction. The transactional attributes are input to the Transaction/Operation which then calls the method to complete the method from the web service running on the server.

Steps for collecting Log data

1. Select all the business critical operations and environment for which logging is to be turned on.
2. Determine the storage for this log data and how long it will be to be stored.
3. Determine the format in which the data will be stored.
4. Determine business users who can access the log data

By applying above steps xml logs can collected for each critical operations are pre-process, parsed and stored in data base. After applying web usage mining algorithm it reveals users who has accessed the web service and how many number of times.

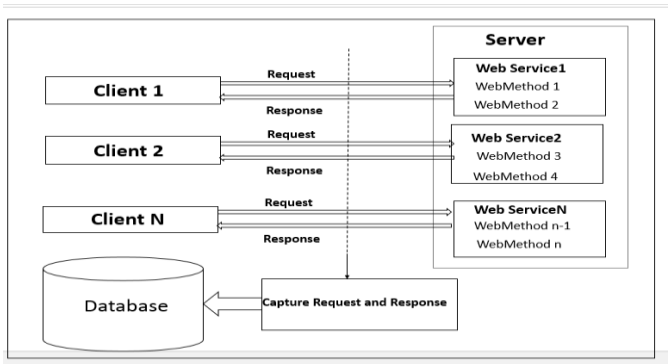

Fig.1. Block diagram of proposed system

Figure.1 shows the block diagram of proposed system where we have integrated Logging module with the Web Service to capture the request and response logs. Here we are writing the request and response logs on to the secure server. Later the system parses the Request and Response Log files and store the business required attributes in to Data base.

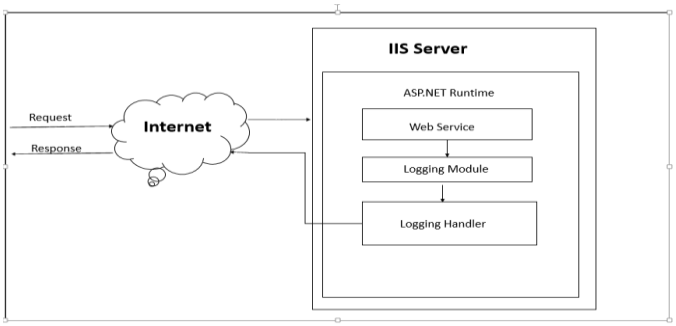

Fig.2. Proposed Logging Mechanism on IIS Server

Figure 2 shows Logging mechanism on IIS server. We can use the different libraries to do the logging. The execution logs are used to mine and analyze Web services usage data. This mining step will help to monitor web service usage by the user. Web Service usage logs collects time series data of web service invocation by business objects, which intrinsically captures patterns associated with industry operations. Web service composition based on such patterns can significantly simplify the business operations [2].

Table I shows Proposed Logged Data Collection Format for capturing the user activity.

TABLE I PROPOSED LOGGED DATA COLLECTION FORMATE

User ID	Web Service Name	Operation	Date	Time Stamp
…	…	…	…	…

E. Web Service logs Mining

Logs offer valuable and significantly important information about systems, networks, and applications. Through audit logs, audit records, and alerts, systems often give signs that something is broken or is going to be broken soon. Logs also reveal larger weaknesses that might affect compliance and even corporate governance. However, system and application logs contain raw data rather than information, and thus require extra effort to be extracted and distilled this data into something useful, usable, and actionable information.

Log records all the events occurring within systems and networks. Audit logs provides activities that may impact the security of systems. It can be in real-time impact or the impact after the event has happened, hence the proper configuration and protection of the logs is very crucial.

Web usage mining is an application of data mining technique which deals with finding out interesting usage patterns from web data, it also helps to understand and serve the needs of web-based applications. It tries to collect and provide meaning to the data generated by the web user's behaviors. While the web content and structure mining uses the primary data on the web, web usage mining mines the secondary data derived from the interactions of the users while interacting with the web [3].

The Security Factors for Logging includes

- Focus: All the system whether they are on premise systems or on-Cloud Systems must have monitoring and logging enabled. Critical systems with no or very less interaction with user may be omitted from scope for monitoring efforts.
- Approach: Validate that logging implementation is in alignment with organizations policies and procedures, especially should be validated in relation with storage, protection, and analysis of the logs.
- Logging Assessment: Review monitoring and logging policies and procedures for defined thresholds and maintenance, specifically for finding any unauthorized access to the web services. Verify that logging mechanism are implemented such that it will send logs to a centralized server, and each logged request and response will bear date and time stamp of activity performed.
- Disaster Recovery: Centralized server where logs are collected should highly available and infrastructure should provide disaster recovery mechanisms.

VI. Conclusion

In this paper a review of Web Service security via Monitoring and Logging is done which is essential to provide complete security on Web service environment. The review of the literature indicates that monitoring and logging along with data mining techniques applied to web service usage logs can provide complete security to system, network resources and web data usage and hence can be used for detecting security violation. . In future work, we will study Filter logs and Escalation logs which contains detail information about the execution of the workflow objects on the server and will apply different data mining techniques to analyze sequence of operations performed by user on server objects.

References

[1] John Steven , Gunnar Peterson, Deborah A. Frincke, Deborah "Building Security In" IEEE SE CURITY & PRI VACY
[2] Vivek R, Prasad Mirje and Sushmitha N "RECOMMENDATION FOR WEB SERVICE COMPOSITION BY MINING USAGE LOGS" (IJDKP) Vol.6, No.2, March 2016.
[3] B.Meena, I.S.L.Sarwani, S.V.S.S.Lakshmi "Web Service mining and its techniques in Web Mining" (IJDKP) vol.2 issue-1 Jan 2014
[4] OverView of Amazon web services April 2017.
[5] G T Raju1 and P S Satyanarayana -"Knowledge Discovery from Web Usage Data: Complete Preprocessing Methodology", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008.
[6] Mohd Helmy Abd Wahab, Mohd Norzali Haji Mohd, Hafizul Fahri Hanafi, Mohamad Farhan Mohamad Mohsin- "Data Pre-processing on Web Server Logs for Generalized Association Rules Mining Algorithm", World Academy of Science, Engineering and Technology 008.
[7] K. R. Suneetha, Dr. R. Krishnamoorthi- "Identifying User Behavior by Analyzing Web Server Access Log File", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.4, April 2009.
[8] M.C. Jaeger, G. Rojec- Goldmann, and G. Muhl, "Qos Aggregation for Web Service Composition Using Workflow Patterns," Proc. Eighth IEEE Int"l Enterprise Computing Conf., pp. 149-159, 2004
[9] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[10] https://docs.bmc.com/docs/display/public/ars81/Logging+and+monitoring+AR+System+server
[11] Guosheng Kang, Mingdong Tang, Jianxun Liu and Xiaoqing (Frank) Liu "Diversifying Web Service Recommendation Results via Exploring Service Usage History" IEEE VOL 9 NO 4 July/Aug 2016
[12] Site http://www-03.ibm.com/software/products/en/qradar-log-manager An American National Standards Designation E 2147-01"Standard specification for Audit and Disclosure Logs for Use in Health Information Systems"

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Ms.Mehdi Tanweer Mehmooda. "Review Paper on Web Service Security and Logging." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017, pp. 61–64.