iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VII **Month of publication:** July 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Implementation of Centralized Logging Feature Using Web Services

Miss. Rohini H[1], Dr. Rajashekarappa [2]
[1,2]*M.Tech in Inforamtion Technology, ISE Department, VTU*

Abstract— Data logging is the technique that involves gathering of log data from one or more applications which produces persistent results at runtime with less effort. This paper describes the server side storage of log data even though logs are generated at clients via a network to a web services .These log data are stored in a centralized database for future references. The goal is to provide ease of implementation to developers and debugging.
Keywords— Operating System, Database, Regular Expression, Web Server

I. INTRODUCTION

The multi tier application is used widely in the software application business worldwide, that implies the use of multiple servers with intensive maintenance. In such cases the applications developers should write code that traces execution steps. This is the condition the logging solution is integrated into the application [1]. An effective solution for logging allows different types of media used for storage and considering different types of log levels for the logged information. The levels of log are successful information, warning, error and debugging. The centralized logging allows detailed processing of requests and performs more accurate diagnosis of the problem. The major interactions for centralized logging are between a client tier, web server tier and database tier. SQL server provides querying and accessing data which is used for storing the log details. The complication of accessing logs increases as the number hosts multiple. Without a good tool searching particular log details of the machine is complex task. A generalized approach to this problem is centralized logging, so that multiple logs can be aggregated in central location. The reformatted log messages are stored in the centralized database, which gives a single point of access and unified view of messages; hence it is easier approach for the distributed systems.

II. LITRETURE SURVEY

In multi tier applications, multiple vendors or open source projects are available for centralized logging. Enterprise Library is the open source logging solutions from Microsoft which is the collection of reusable software components. A straightforward methodology is to setup record replication of logs to a focal server on a cron plan. Typically rsync and cron are utilized since they are basic and clear to setup. This arrangement can work for some time yet it doesn't give opportune access to log information. It additionally doesn't total the logs and just co-finds them. The syslog has two executions [2] such as rsyslog or syslog-ng. These daemons allow techniques to send log messages and the syslog arrangement decides how they are put away. In an incorporated logging setup, a focal syslog daemon is setup on system and the customer logging daemons are setup to forward messages to the focal daemon NLog allows logging to files, windows event log, network, database, web services and other sources [3]. Web services allow communication via SOAP, HTTP GET and POST, along with the security via HTTPS.

III. METHODOLOGY

As this improvement was made to be utilized by multi level applications, and as multiple tiers can be reduced to 3 tiers by grouping the layers that can exit in the same machine, it has a 3 levels structure. The application includes the client layer, the web server layer and the database layer. For every layer there is at least one assembly that needs to be conveyed and designed. The log message is asynchronously posted to the Log module from the distinctive target machines with the timestamp without waiting for the acknowledgment. Log Module is a Message buffer container, the log message from the objective machine are gathered and stored. The size of the buffer is different based the quantity of messages gathered from the diverse target machine.

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

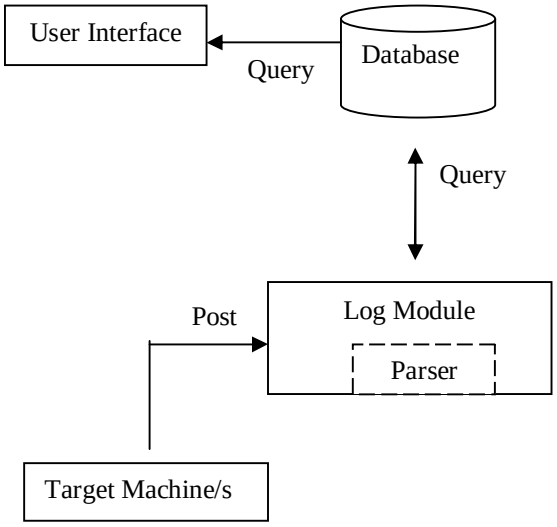


Figure 1: Architecture for Centralized Logging

The received log message from the Log Module are parsed and stored to the database. Parser processing plant is considered for the distinctive source. The parsers are chosen taking into account the source got amid the trigger for establishment.

If failure occurs (response has not been received): The failed block of messages are appended with next block of messages and sent to the Log Module.

A. Flow Chart

The flow of information communication between the tiers is sequential meaning data will emerge from higher level and lower level will process it. The logging data can be generated at any level and later it should be passed to a data collection service.

The information is generated and passed to data collection service by the client tiers. The logs are correlated from clients and servers with the web server tier. Logs are sent directly from server to database tier.

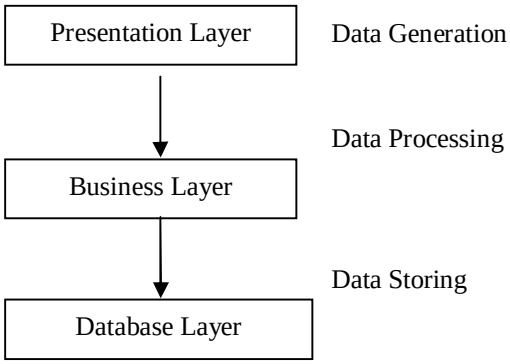


Figure 2: Multi –tier data flow architecture

The data flow has three important steps

The data generation

The data processing

The data storing

The client side and server side is located by the data producers. The data is processed at server side and stored in the database. The client side target machine takes logging data details and post it to the web service.

The presentation layer consists of TargetMachine class, which is used to post details to the web service in the business layer.

The business layer i.e web server contains the classes responsible for the initialization of database layer, data management and logging target at server side.

B. Class Diagram

The LogModule is the class the implement most of the functionalities of web services with ILogParser interface for parsing the posted by client. The database layer is comprised of the database server application with tables and stored procedure for log management. Linq is used as object-relational mapping engine, insertion is done through store procedures which are used to separate log information and store in corresponding tables i.e tbl_details.

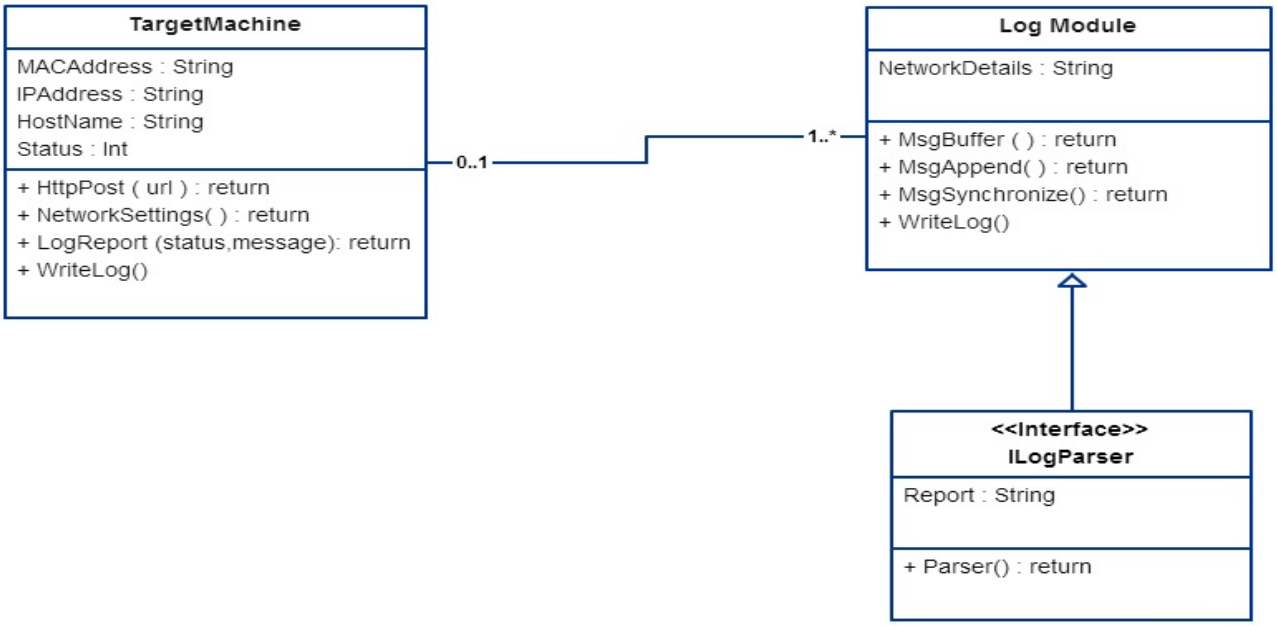


Figure 3: Class diagram of assembly contents

C. Log formatting

Log formatting is used to extract the fields needed for mining the log database algorithms to get rid of garbled logs from the source logs. In this paper regular expression is used to format logs before mining the logs.

Pseudo code for matching Regex

```
Define regular expression that match log format
while(read log message from file)
if(not the end of log file)
    if(expression match the log file)
            Read the messages;
            Store into the central database;
    else
            Do nothing;

     end if
  end if
 end while
```

The regular expression is used for verfiying the common operation for storing the log messages.If expression matches then the logs are stored to the database else do nothing till the expression matches .

Pseudo code for timestamp comprasion of messages

```
Define time threshold T;
 timestamp of machine;
while(get next log message)
```

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

```
if(is end of file)
    break;
else
    old timestamp – current log message timestamp;
        if(failure of message)
            Append with last message ;
        else
            Store the message;
        end if
  end if
end while
```

The system log format is composed of log timestamp,log occurance of the node,log inforamtion description etc. The old timestamp of the machine is compared with the new timestamp ,based on this the messages are stored to database.

IV. LOG ANALYSIS

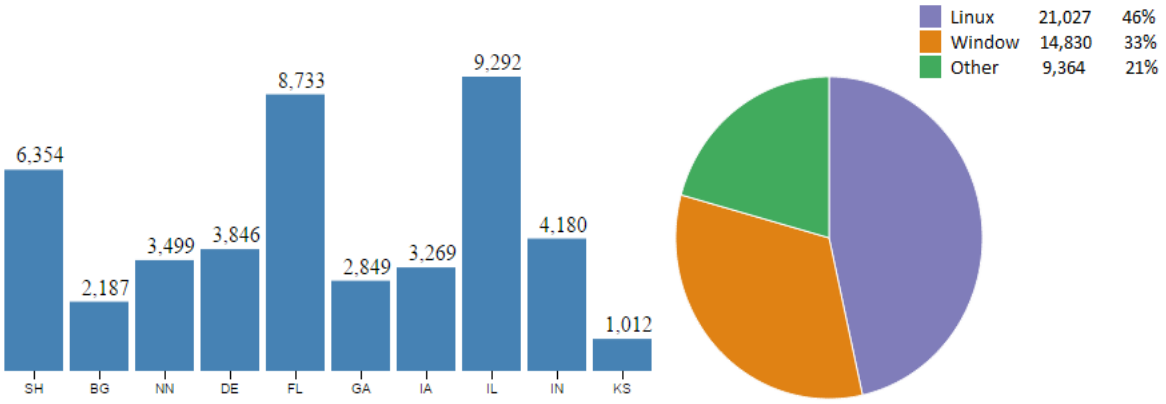


Figure 4: Messages in database

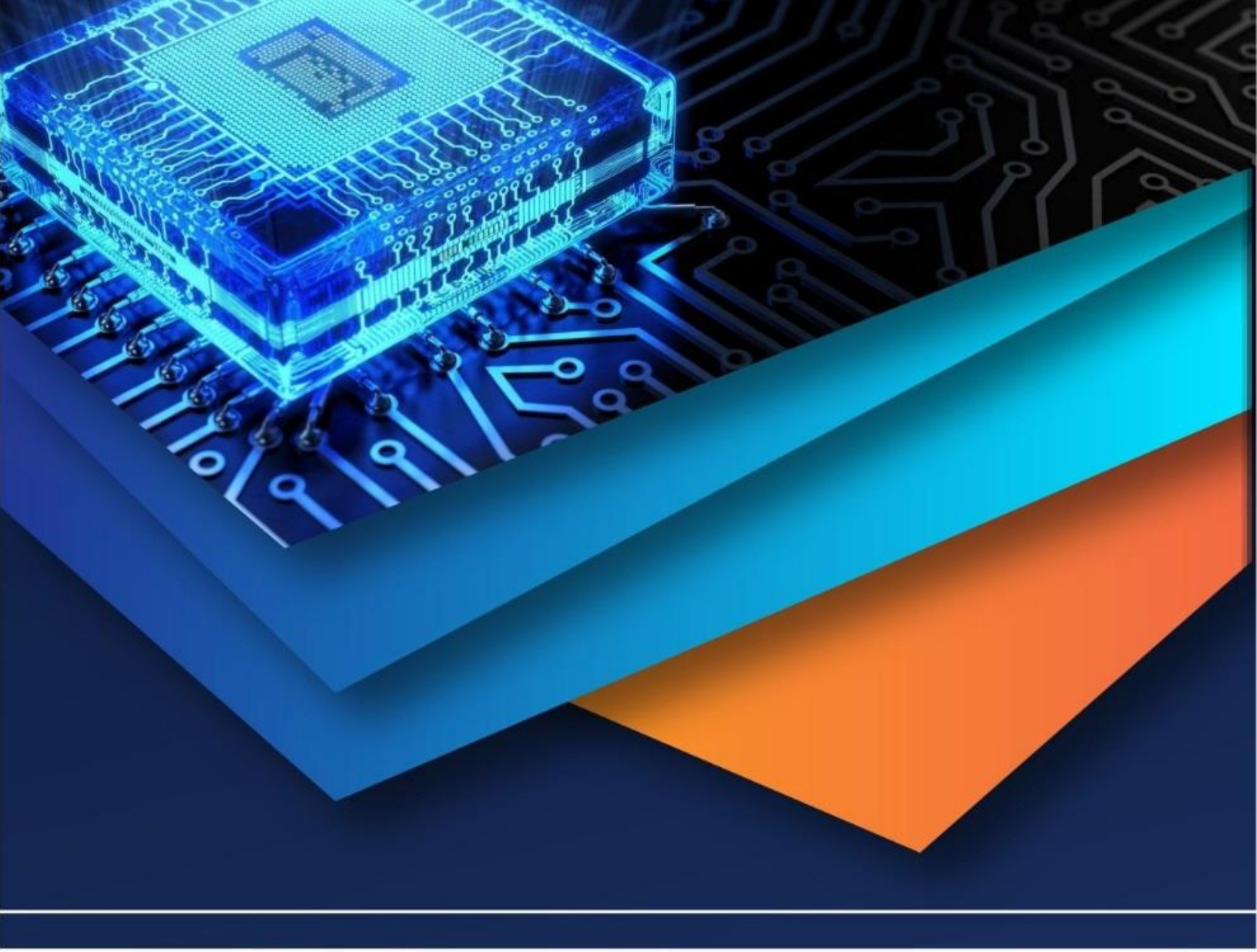
V. CONCLUSIONS

The application contains the most well-known 3 levels it is conceivable to perform integration with complex structures. The framework structure will furnish us with focal administration of secure logging through a web administration. Since the application execution is controlled by framework it is more improbable for an engineer to confer a mix-up at the point when enlisting our objectives in the framework.

One of the greatest preferences over traditional document or support logging is the capacity to perform described detailed query on the data we have accumulated. Since we store the logs in one location we could screen the event of certain use designs in customer applications.

REFERENCES

[1] B. Sang, J. Zhan, G. Tian, “Decreasing log data of multi-tier services for effective request tracing,” Institute of Computing Technology, Chinese Academy of Sciences, CN, 2009.
[2] Anand Deveriya. An Overview of the syslog Protocol[M]. Cisco Press, 2005.
[3] J. Kowalski, http://nlog-project.org/home, 2010
[4] S. Dragoş, M. Ureche, “LogMonitor – W3C log file format monitoring tools,” Novice Insights, vol.4, Technical University of Cluj-Napoca, 2008.
[5] C. Cwalina, B. Abrams, “Framework Design Guidelines”, Addison-Wesley, Boston, 2009.
[6] J. Lowy, “Programming WCF Services”, O’Reilly, Sebastopol, 2007
[7] D. Comingore, D. Hinson, “Professional SQL Server 2005 CLR Programming”, Wiley Publishing, Indianapolis, 2007.
[8] J. Myers, M. R. Grimaila, and R. F. Mills. Log-Based Distributed Security Event Detection Using Simple Event Correlator[C]. System Sciences (HICSS), 2011 44th Hawaii International Conference, Date:4-7 Jan. 2011.
[9] K. Fukuda. On the use of weighted syslog time series for anomaly detection[C]. Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium, Date:23-27 May 2011



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY