ISSN No:-2456-2165

Security Log Analysis

Based on Big data

Allenki Shiva Santosh
Institute of Aeronautical Engineering IARE
Hyderabad, India

Abstract:- Brutal cyber attacks these days tend to shut down the control systems of all companies and prolonged use of this results in a cyber war. Urge of new security system is required in today security management which is called as Enterprise security management ESM which is a integrated network system comprises of firewall, internet protocol etc. The present security management system has capability of shielding the data from outside sources and all the traffic inflows from outside to inside. The security system suggests that intelligence of security by determining the relation between security and data events from the network system. This mechanism is done by Big data. It also applies Distribution based technology through the security log system. This attacks include active attacks, passive attacks, SQL injection attacks.

Keywords:- *Big Data, Log analysis, Security, Cyber attack, Trojans and Malwares.*

I. INTRODUCTION

The Advanced persistant Threat introduced new alignments in the machine code by different way of attacking which is primarily used as a attack weapon in the past .Counter attacking the Apt becomes difficult as it achieves the goal by using whole possible after securing information of the target.

In the past, cyber-attack was a random way of attacking, but these days it emerged as an idol of attacking. Recently hackers choose long term attack type by cooperating to know weakness of the target and also more and more companies are increasing day by day with these Apt attacks like Hyundai.

It is important to have a security management system which includes In system security like Firewall and protocols and to prevent the flow of data to thefts. Current security system collects logs and saves it in database system and present condition on screen after analyzing the saved data. It sends an immediate message at the end to the manager if there is any problem. But the current security system only blocks cyber-attack from outside because it has network based attack method. It only collects log condition of systems and event condition individually which are occurred presently. It emphasis to describe and enhance the application.

Hence the security log analysis using Big data increases the level of security and notifies the manager who the attacker is.

In this research, I would like to describe and mention and analyze the Massive amount of structure - unstructured data by distributed saving technology through security log analysis using Big data Analytics. I would also like to suggest that real time monitoring by distribution based searching. I believe that this type of security system brings new change in managing the log analysis and to shield data.

II. RELATED THEORY

Security Management is for level of security to integrate control management, which includes remote mechanism of security management. The earlier researchers found that firewall and protocols were absent as a result data can be interpreted from the inside sources. But still theories suggests that it's difficult to prevent the Apt attacks as a result of performance and database management which has large amount of data.

This includes all the functions of current security management which give detailed analysis of unknown threats by using total analysis. With the acquisition of large amount of Data which include structured and unstructured security can be controlled.

To make a new security integrated mechanism worth, a analysis mechanism has to be enhanced which gives the relation between security events and data from network systems. Security Information and Event management will be the Next big thing in the security World as the new generation security analysis technique.

III. DESIGN OF SECURITY LOG ANALYSIS USING BIG DATA

A. Information calculating Platform

Information processing is performed of analyzing, saving and optimized blocks of data. Each function has various formats. This platform collect data constantly from many data sources, and save data constantly by many parallel structures, offer the system structure that is able to analyze efficiently based on Fast processing.

B. Designing the program for Collecting Big Data

In designing the program one should consider all data collecting techniques including data transmission and also stability of the data and engaging the data. The information designed and prepared in stored in Real time in collector through transmitter. The present data collecting process shows the quality of the analysis in web home pages. It is recommended to use agent collecting information and another without agent collecting information. These add flexibility to the collecting methods. Data transmitter sends error and load of data, and prevents loss of data by automatically load distribution. There is a program for data collecting by integrated data collector.

Huge amount of liquid data is send from the system which is done by interlocking adapter and system performance

adapter with UNIX performance by applying technology of User datagram protocol packet technology. To transmit the collected data from the adaptor, which is performed by verifying data and adjusting transmission volume by equipment. In case of data overflow, the data transmission doesn't takes place. If error occurs during the process, data should be saved and repeated process of the data with SSL certification, LOG filter functions. Usage of Mechanism to save the Big log file saves in the system.

C. Data Reducing Module

Collector module is developed by Distribution servers. Also a saving mechanism is available for collector server. The data arriving from the collecting system is made for clients to find the information through receiving and normalizing process, compared with normalized data system, and obtain index value with DB. The data of security log, application log is received and it is normalized through normalizing engine and data tagging. Use distributed Mechanism to save the Big security log file. The divided architecture is processed in parallel processing to store Big data, and runs saving and real time index work by distribution multi indexer. Here the Tera byte (TB) data can be processed by the divided architecture, and each collector shows 200,000 EPS performance per day. Including the each collector basically checks when saving data, and saved data in compressed and encoded folder. The collectors generally backup and restore by constructing data backup/hot spare collector to protect the original data automatically from possible defect of multi system. Analytically this structural management can store unlimited data. And has high flexibility. This technique can make a significant way to process security log file when the data size is reduced.

D. Data Analyze Mechanism

The vulnerability speed of Big data cannot be guaranteed by checking in real-time. It can be found out by imposing the keywords in the collector. The information from the security equipment is checked the real-time performance are of two types distribution scanning. One is to detect rapid changes in data based on baseline and the other threshold value .The next one is usage of trending analysis based on data statistics.

The analysis of all the particular events which are in the diagram by real time monitoring of movement of other users of the data. An alarm is set to define a threat when an error is observed in real time monitoring system. To utmost two billion of single scans are run over the time for a day.

E. Log Structure in Big data analysis

All the data structures must be constructed in considering the data techniques including Big data, stability, and high consistency for data collection. Hence the formatted data log data source from security equipment are collected and stored through transmitter.

F. Algorithms

On basis of my observation, I would recommend using Perl Adaptable Mechanism which is a process or program which increases the mode of separator analysis for unstructured data.

This program is to find the number of logs which are separated into the log server, which includes, log parser, log transmission. Log collecting server passes the collected data to the log filter by using equipments like protocols and Firewalls.

IV. CONCLUSION

I've designed and prepared data and processed it accordingly based on information analysis using Big data. As the next Big thing is Data shielding saving Big data emphasis expandability and availability of security logs.

During this research particular area of the Data science is considered and researched. This techniques of data analyzing can be applies to all areas of the Big Data like Robotics, manufacturing.

V. ACKNOWLEDGEMENT

I thank all the referrers for their useful and Worthy suggestions the majority of the work contained in this paper was completed as part of the author's Research work in Data science.

REFERENCES

[1]. L. Seung Ha, K. Seung Won, K. KiHong, P. Sechung, " Design of Big Data ETL Model for Aggregating of Security Log/Event ", KICS, (2014).06.
[2]. M. Nicolett and K.M. Kavanagh, "Magic Quadrant for Security Information and Event Management," Gartner Group, (2012).05.
[3]. K. M. Kavanagh, M. Nicolett, O. Rochford, "magic quadrant for security information and event management", Gartner Group, (2014).06.
[4]. M. Nicolett and J. Feiman, "SIEM Enables Enterprise Security Intelligence," Gartner Group, (2011).01
[5]. M. Nicolett and K.M. Kavanagh, "Critical Capabilities for Security Information and Event Management," Gartner Group, (2012).05.
[6]. N. MacDonald, "Information Security Is Becoming a Big Data Analytics Problem," Gartner Group, (2012).05.
[7]. J-s Yun, H-s Kang, I-y Moon,"Analysis study of movement patterns using BigData analysis technology", Journal of Information and Communication Convergence Engineering, vol.28, no.5, (2014).