ISSN 1533-9211

DOI 10.5281/zenodo.6827467

SECURITY FOR CLOUD-NATIVE SYSTEMS WITH AN AI-OPS ENGINE

PAVAN KUMAR[1], KRISHNAPPA H K[2] and PETER CHACKO[3]

[1]Student at Department of Computer Science and Engineering, RV College of Engineering, Bengaluru, Karnataka, India.Email: pavankumarck.scs20@rvce.edu.in
[2]Professor and Associate Dean at Department of Computer Science and Engineering, RV College of Engineering, Bengaluru, Karnataka, India.Email: krishnappahk@rvce.edu.in
[3]Founder and Director, Organization: Neridio System, City: Bengaluru, State: Karnataka, Country: India. Email: peter@neridio.com

Abstract:

Cyber security is referred to the process, technologies and practices for protection of devices, networks, and data from damage and unauthorized access. Cyber security has always been important because military, government, financial and corporate organizations collect, store and process enormous amounts of data on computers and on the other devices. As the older threats are eradicated, newer threats are being added to the system by the adversaries. This project is aimed to provide a secure communication between a server and a client. Many cryptographic libraries are available for this purpose but many libraries do not have adequate documentation.

Now days it is necessary to monitor and regulate the data security systems for controlling unauthorized access and many of the attacks. Intelligent Vault is a cyber-security tool to protect and monitor the available data. In the way of 360-degree security in automation, surveillance, Storage Intrusion Threat Intelligence and Real-Time Response through its Intelligent Vault. It sync's the data from the proxy systems. The data processing will be performed in R-client and R-server using Nervio-Guard package. Telemetry validation and Real time processing of Advance SecOps will be processed in Intelligent Vault

Keywords: Artificial Intelligence, Machine Learning, Rational-Client, Rational-Server

A. INTRODUCTION

Cyber security is to protect any system, program, or a network from attacks that are digital. The main objective of a cyber-attack is to access, modify or destroy information such as stealing money from users or interrupting businesses. An implementation of cyber security has become a major challenge since there are a huge number of devices when compared to people and that attackers are using different techniques to launch attacks.

The proposed work is mainly focuses on building the vault which provides protection from many Ransoms ware attacks and constant monitoring and also protects the data in private cloud. The number of clients can be connected to server and configuration and software updating from server to client are checked and status is updated. Various required features like Remote command execution and custom command execution are incorporated.

This chapter describes the introduction and overview of how data is monitored through Intelligent Vault.

DOI 10.5281/zenodo.6827467

B. RELATED WORK

This section presents literature review on several research areas related to Intelligent Vault for Cyber Security and Cloud Based Security. Verifiable and Secure SVM Classification for Cloud-based Health Monitoring Services

1. In this research it shows that VSSVMC is extremely efficient in terms of computation, communication and VSSVMC achieves microsecond-level execution time with kilobyte-level communication and storage overheads on the tested dataset. A Review of Cloud-Based Malware Detection System: Opportunities, Advances and Challenges
2. In this research explains advantages and disadvantages of cloud environments in detecting malware and also proposes a cloud-based malware detection framework, which uses a hybrid approach to detect malware. Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security
3. In this research number of ML algorithms are used to predict Spyware/Ransomware and spear phishing. We have recommended relevant controls to tackle these threats and advocate using Cyber Threat Intelligence (CTI) data for the ML predicate model for the overall Cyber Supply Chain (CSC) cyber security improvement. Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances
4. In this research we have presented an overview of recent advances on the physical safety and cyber security issues of Multi-Agent Systems (MASs) and presented the results on physical fault estimation, detection and diagnosis, fault-tolerant control, cyber-attack detection, and secure control under two typical kinds of attacks: the DoS attack and the Deception attack. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid
5. In this research they have explored various threats and vulnerabilities that can affect the key elements of cybersecurity in the smart grid network to maintain and develop a strong physical architecture for the smart grid, and then present the security measures to avert those threats and vulnerabilities at three different levels. Research on key technology of Network Security situation awareness of private cloud in enterprises
6. The paper concentrates on network security situational awareness of private cloud in the era of big data and analyses the relevant evaluation indexes. Cloud Threat Defense - a threat protection and compliance solution
7. This paper explores the security issues related to clod computing and proposes a cloud native scalable security solution for the cloud. Security Assessment of open stack cloud using outside and inside software tools
8. The paper provides security analysis for private cloud solution open stack. Various security threats found on multitenant environments can be provided with concrete solutions for each situation. Critical Security issues in Cloud Computing: A Survey
9. This paper focusses on variety of security issues in cloud computing and accomplishes a survey that addresses cloud security which includes computer, Network and Information Security. Cloud Security Ecosystem for Data Security and Privacy
10. The paper focusses on creating a secure cloud ecosystem by making use of multifactor authentication along with multiple levels of hashing and encryption

III. KEY TECHNOLOGIES

A. Sending Logfiles to server

All the events performed by the user are maintained in log files, Log files sync automatically with the servers. These files provide administrators with a detailed information to find the root cause of problems and troubleshoot errors. Log storage are scalable to suit organization's expanding needs and periodic surges in log volumes. Log analysis involves parsing logs details into different categories, analyzing the data to define baselines, visualizing the data using different graphs, and understanding regular patterns and anomalies

B. Configuration updating from server to client

The issues facing by the user were raised in the community or application technical teams. These are troubleshooter by the technical team in backend and will update the bugs and patches this was sent to sever to communicate back to user as configuration update.

C.Software updating from server to client

As the generation passes, a certain change needs to make as to be updated in the market. The bugs and errors faced by the users are recorded and fixed, the overall updates and the additional features included and made a package and sent to user as new version update.

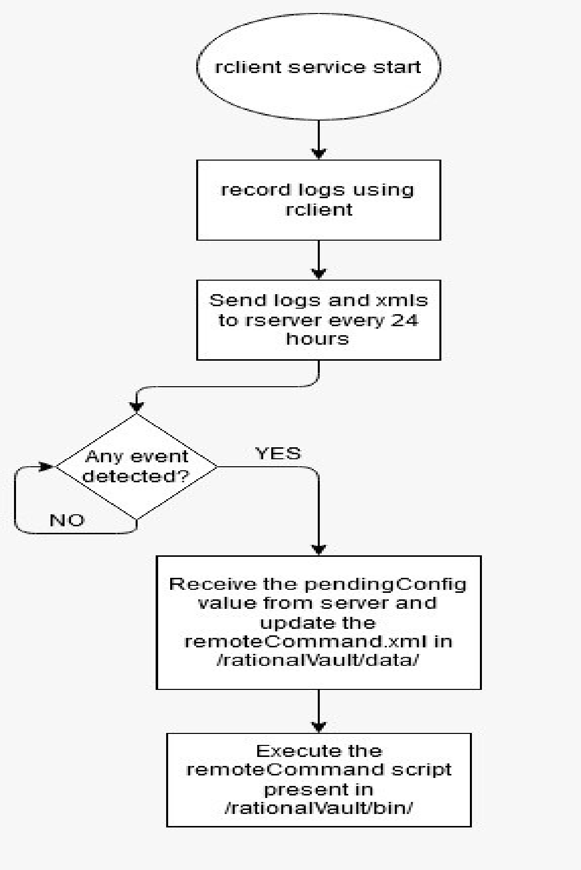
D. Remote Command Execution

In a group of LAN networks, the user is strictly to access few objects and sites which are into the working modules. If the user tries to cross the limits and restrictions, then it will be easily identified by admins, as intern they work on remote command execution to halt the process and access of the entities, which are not allowed by the organization.

IV. PROPOSED METHODOLOGY

This section explains the methodology of the project to provide a working of R-client and R-serve

DOI 10.5281/zenodo.6827467


rclient service start
record logs using rclient
Send logs and xmls to rserver every 24 hours
Any event detected?
YES
NO
Receive the pendingConfig value from server and update the remoteCommand.xml in /rationalVault/data/
Execute the remoteCommand script present in /rationalVault/bin/

- R-client is a client user interface and processes the requested functions to perform.
- R-server performs the operations based on the inputs from R-client.
- In R-Server, we are introducing our own protocol stack DDP (Data Distribution Protocol) for Real-Time Response through its Intelligent Vault.
- As a part of working intervals, a system logs will be generated.
- Here, we have implemented reaction response through remote command delivery and Multiple
- Features of SecOps were integrated by verification code for tracking the features of custom security commands, which were generated in logs file.
- R-server monitoring the verification code for tracking the features of custom security commands and continually monitoring the R-Client workflow to ensure real-time file scans and it invokes the specified command using AI (Artificial Intelligence).

ISSN 1533-9211

DOI 10.5281/zenodo.6827467

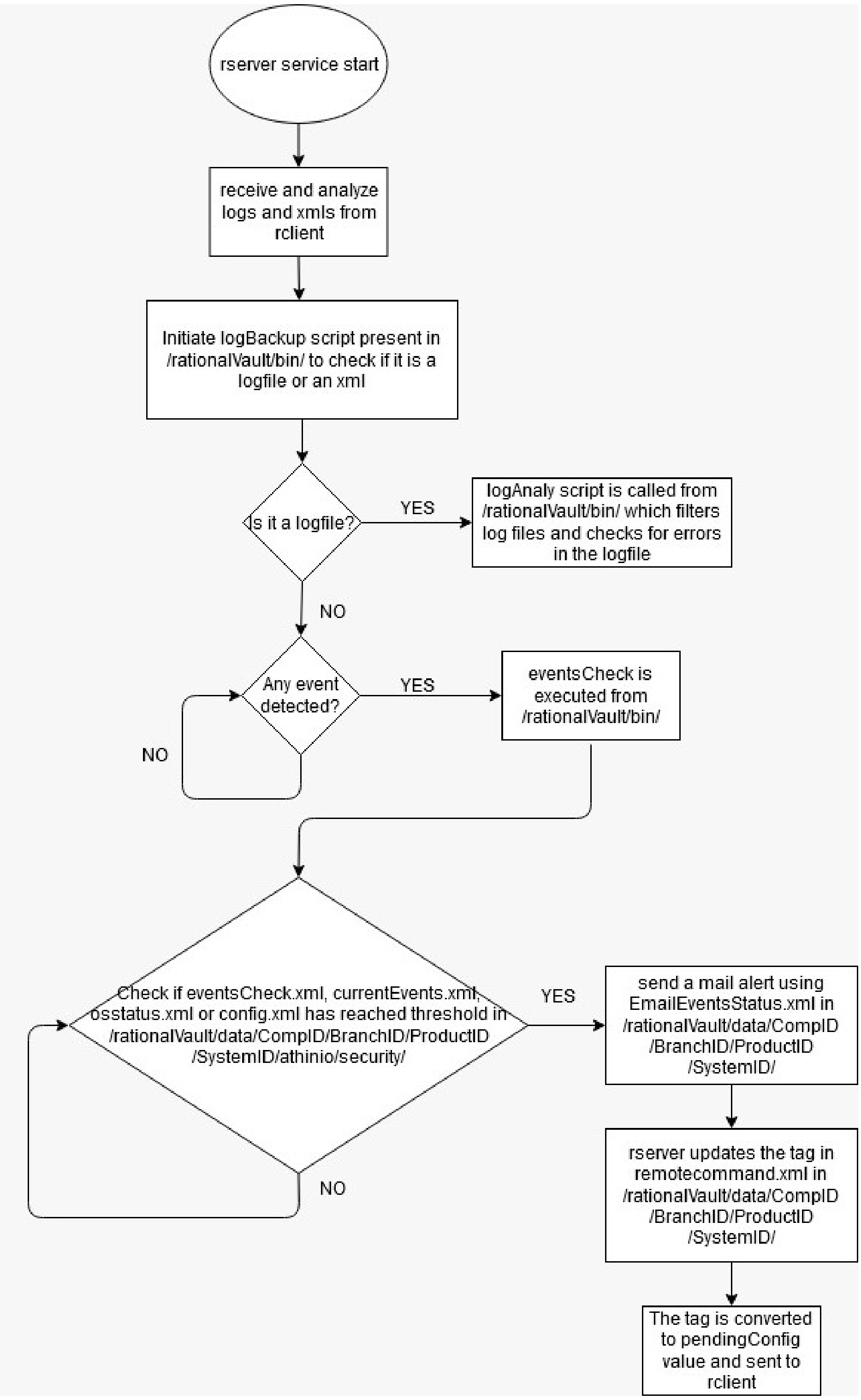

rserver service start
receive and analyze logs and xmls from rclient
Initiate logBackup script present in /rationalVault/bin/ to check if it is a logfile or an xml
Is it a logfile?
YES
logAnaly script is called from /rationalVault/bin/ which filters log files and checks for errors in the logfile
NO
Any event detected?
YES
eventsCheck is executed from /rationalVault/bin/
NO
Check if eventsCheck.xml, currentEvents.xml, osstatus.xml or config.xml has reached threshold in /rationalVault/data/CompID/BranchID/ProductID /SystemID/athinio/security/
YES
send a mail alert using EmailEventsStatus.xml in /rationalVault/data/CompID /BranchID/ProductID /SystemID/
NO
rserver updates the tag in remotecommand.xml in /rationalVault/data/CompID /BranchID/ProductID /SystemID/
The tag is converted to pendingConfig value and sent to rclient

Figure 2: Flow Chart of Working of R-Server

DOI 10.5281/zenodo.6827467

V. IMPLEMENTATION DETAILS

This chapter provides the implementation details for establishing a secure connection between two parties.

A. Programming Language Selection

Programming language is set of rules for a computer to perform a specific job. There are a number of programming languages such as C, Shell script, Python, PHP, jQuery. Which are high-level programming languages. A high-level language is considered to be closer to human language.

The project makes use of C programming language. The SCA which uses the openSSL cryptographic library is written in C language.

B. Platform Selection

The following section provides details of the software platform used for executing the project.

C. Operating System

System software managing software resources and hardware of the system is known as operating system. The project has been carried out using CentOS Stream. 7-2009, which is an open-source Linux distribution.

D. CMake

A CMake is software to manage building process that uses a compiler- independent method. It has been designed to support hierarchies in directories and applications which depend on multiple libraries. CMake can be used in combination with build environments like Apple 'sXCode, make and Microsoft Visual Studio.

Considering a number of directories which contains the source code and the header files, CMake takes care of all the dependencies, build orders and required tasks before the project is compiled. It is not responsible of any kind of compiling tasks.

E. Configuration of R-Server

This section describes the configuration of rServer and secure communication to take place between two hosts i.e., rServer and rClient.

The R-Server starts getting the logs and xmls from client side, by using log backup script we can identify the whether it is logfile or XMl file. If it is logfile then logAnalyze script will be invoked and it checks for the errors in the logfile and if any event is detected then it will check the threshold limits, if threshold limit is exceeded then rServer will send a mail to the admin regarding reached threshold limit and admin will set the command in Cmd_in.xml and tag is converted to pending code value and sent to r-client (based on the command, the script will be run on the client side.

DOI 10.5281/zenodo.6827467

F. Configuration on R-Client

This section describes the configuration of rClient and secure communication to take place between two hosts i.e., rClient and rServer.

In R-Client, all logs are generated and it is stored in xml file and it is sent to R-Server and it'll be checking the logs every second and it'll be monitoring the system every 24hours. If any error is detected from the client side, then it'll receive the pending code value from the R-Server after that it'll update the value to the particular XML file and showing error to the particular client from the assigned hierarchy.

Summary

This chapter provides the details of the programming language, platforms utilized and the difficulties encountered during the execution of the project.

VI. EXPERIMENTAL RESULTS

This chapter discusses all the results that were obtained during the implementation and testing phases. It also discusses about the final output that is being obtained and the performance of the Functional Test Infrastructure.

A. Result Analysis

Test cases run on the secure infrastructure shows that the performance of the infrastructure has increased. Hence, the approach of setting up Intelligent Vault helps to secure the computer system and automation infrastructure resources of the organization and provide stability for the IT operation.

B. Security-At-Rest For Data Protection

In the Security-at-rest it is used for data protection at rest aims to secure inactive data stored on any device or network. Data at rest includes both structured and unstructured data. This type of data is subject to threats from hackers and other malicious threats to gain access to the data digitally or physical theft of the data storage media. To prevent this data from being accessed, modified or stolen, organizations will often employ security protection measures such as password protection, data encryption, or a combination of both. The security options used for this type of data are broadly referred to as data at rest protection using our advanced security commands for monitoring the file system.

C. Ai Security Policy Management

In the automatic remote command execution if it exceeds the user given threshold limit (some of the events are based on the user system specification) then it executes the specified action for the particular events.

In the security policy management, it is used to identify the ram, storage, running process of current running status of the user system and data activity report for identifying the attack detection and specified command is executed.

D. Fault And Threat Dashboard

In the fault and threat dashboard for getting system logs from that we are detecting if there any threat detection is detected or someone is trying to access or any software or script is injected then the logs will be displayed in the threat dashboard.

In Alert Management section, all the ram, storage, running process of current running status of the user system events will be display for the particular user for the assigned hierarchy to display the alert messages for the particular events

E. Advanced Telemetry Dashboard

In the system general statics, logged-in user information and top 10 processes (sorted by virtual memory usage) logs from that we are displaying the how many running processes in the system and while running processes it'll take some memory, that memory will be displayed and how many users are logged in and what time users have been logged-ON all these information will be displayed in the view dashboard.

Summary

This chapter summarizes the results generated from testing scripts on Infrastructure and also summarizes the results after fetecting all the system generated logs. It gives the analysis on the performance of the infrastructure after installing this software package.

VII. CONCLUSION

The security monitoring provides a secure environment for data transfer. Controlling critical infrastructure systems is the role of human operators. Here the security monitoring in the market is growing day by day, as the cyber-attacks and threats are increasing. The Literature survey is conducted rigorously to identify the various existing security monitoring methods and their drawbacks are identified as research gap.

Our main objective is to design intelligent decision support systems to enhance the decision-making capabilities of operators (considering the overwhelming number of alarms that are typically received after a fault and the associated short response time required) and to assist them in normalizing the state of art of systems at all times. Intelligent decision support systems are capable of processing real-time sensor information, to provide high-level information to human operators in a way that can be easily understood and visualized. Further we need to define methodology to meet the defined objectives.

REFERENCES

1. Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. Energies, 14(18), 1–22.

2. Aslan, Ö., Ozkan-Okay, M., & Gupta, D. (2021). A Review of Cloud-Based Malware Detection System: Opportunities, Advances and Challenges. European Journal of Engineering and Technology Research, 6(3), 1–8.

3. Sen, J. (2018). Security and privacy issues in cloud computing. Architectures and Protocols for Secure Information Technology Infrastructures, iv, 1–45.

4. Liang, J., Qin, Z., Xue, L., Lin, X., & Shen, X. (2021). Verifiable and Secure SVM Classification for Cloud-based Health Monitoring Services. IEEE Internet of Things Journal, 4662(c), 1–14.

5. Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. IEEE Access, 9(Ml), 94318–94337.

6. Zhang, D., Feng, G., Shi, Y., & Srinivasan, D. (2021). Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances. IEEE/CAA Journal of Automatica Sinica, 8(2), 319–333.

7. Gordin, A. Graur, A. Potorac and D. Balan, "Security assessment of OpenStack cloud using outside and inside software tools," 2018 International Conference on Development and Application Systems (DAS), 2018, pp. 170-174, doi: 10.1109/DAAS.2018.8396091.

8. X. Sun, "Critical Security Issues in Cloud Computing: A Survey," 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), 2018, pp. 216-221, doi: 10.1109/BDS/HPSC/IDS18.2018.00053.

9. Arora, A. Khanna, A. Rastogi and A. Agarwal, "Cloud security ecosystem for data security and privacy," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, 2017, pp. 288-292, doi: 10.1109/CONFLUENCE.2017.7943164.

10. Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C.-W. (2021). Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing. IEEE Access, 1–1. doi:10.1109/access.2021.3049564.