

Cloud Security Issues and Log-based Proactive Strategy

Oumayma Mejri*, Dana Yang**, Inshil Doh*

*Dept. of Cyber Security, Ewha Womans University

**Dept. of Computer Science and Engineering, Ewha Womans University

oumaymamejri@gmail.com, yangzzzzzz@ewhain.net, isdoh1@ewha.ac.kr

Abstract— Recently, given the current situation the world is undergoing with the COVID-19 pandemic, a lot of companies encourage remote working from home. As a result, the use of the cloud has increased, but as a consequence, cyberattacks on the cloud systems have escalated. However, organizations and companies still have concerns about the use of the cloud as most of them remain unaware of the security threats against cloud system. This work researches through major concerns of the organizations and companies for cloud security and tries to explain why it is important for the organization to be aware of the threats that the cloud is facing. It also proposes a three-step strategy to help companies and organizations to secure their cloud system.

Keywords—Cloud, Cloud computing, cloud security, Log management

I. INTRODUCTION

Nowadays, computers, printers, dedicated firewalls, routers and countless other devices featuring a network interface do not only generate more system log but are also capable of sending the logs over the network to pre-configured destinations. As the number of devices on an administered network grows over time, it is becoming less likely possible to monitor and analyze on a per-device basis, and it would not be efficient and can be time-consuming. Event logs play an important role in modern IT systems since they are an excellent source of information for monitoring the system in real-time and for conducting retrospective event analysis. Logs are a critical part of any system, and the information they provide about any application is vital and can answer questions on what the system is doing and what has happened. Computer data logging is the process of recording information about events that occur in a computer system. The output of logging is a set of log entries where each one includes the characteristics of an event together with an associated time value. Logging information can among others be used for traceback, event reconstruction, and discovery of digital evidence. When the system is hosted on one machine, file logs are easy to access and analyze, but when the system grows to multiple hosts, log management is becoming a nightmare[1]. It is difficult to look up a particular error across thousands of log files on hundreds of servers without the help of specific tools. A common approach to this issue is to deploy and configure a centralized logging system so that data from each log file of each host is pushed to a central location. It is very challenging for engineers to find the right tool to manage their

logs, as logs are a very crucial point in any network or system, they help with saving time for troubleshooting.

Recently cloud providing service companies are a target of attacks. Cloud service attacks have been increasing recently, as the attackers are trying to gain access to major corporate accounts, or simply try to manipulate or acquire normal people's sensitive data. With the recent situation the world has encountered with the COVID-19 pandemic, major companies, universities and small companies have resorted to working from home and consequently have been forced into using cloud-based tools. Mostly the employees or students will have to access these services remotely using a web browser, so basically, the attacker would have better chances to lead a successful attack. According to "McAfee" company, the attacks targeting cloud services have risen by 630percent since the start of the pandemic[2]. So the question remains, Should companies rely totally on the cloud company without monitoring their own data?

In this paper, we have proposed a log management framework that consists of several steps, which can help organizations to have better control over their own system, and to better secure it against the spreading attacks on the clouds. This framework consists of mainly three different steps that can help better secure the system. The first step is setting a solution to do a complete scan to detect any miss configuration in the system, the second step is to integrate a vulnerability scanning tool, and the last step is to monitor and analyze the logs using a log management solution.

II. RELATED WORK

A. Motivation and related research

In the cloud there are a variety of shared resources that pose a lot of issues. Most importantly heterogeneity[3] has discussed the challenges in cloud computing by analyzing different types of heterogeneity in cloud computing systems by taking a lot of factors as considerations. Heterogeneity imposes a lot of challenges such as job scheduling, data and task placement, resource sharing, and resource allocation. They have been addressed by highlighting the promising existing solutions that addressed each challenge. As stated, even a lot of state of the art research has been done to address

the challenges, the problem still sustains and the field is open to more research.

As the use of the cloud is increasing so have been the attacks and the common attacks are DoS and DDoS, [4] studied the increase of DoS and DDoS attacks on the cloud and its impacts in the cloud by listing the procedures used by the attackers to perform their attack on the cloud, an important issue is what preventions need to be taken to lessen the severity of these attacks in the cloud. Simulations were done on a private cloud, and the results showed the techniques discussed to lessen the severity of the attack does work, however, nowadays, attackers acquire more advanced tools to help them with their attacks so more detailed research remains to be done. With the advances attackers have made recently, more measures should be taken to secure the cloud.

According to a research[5] from CIO(Chief information officer) Research Center Report, constant concern for CIOs when it comes to the cloud is the security of the cloud. The authors recognize the biggest three security threats for the cloud are XML signature, Browser security, and Vendor Lock in. The paper further discussed and investigated security attacks and threats in the cloud and listed some solutions that can be used to secure the cloud. Security threats have been discussed in detail and possible existing approaches for each threat have been listed.

B. Log management framework

As mentioned before the amount of data that is being generated in the cloud is under constant threat of being manipulated or stolen. Therefore, organizations need to take measures to protect their data and resources in the cloud. The right approach starts with choosing the appropriate log management solutions to manage the data or resources. When a breach happens in the network, there is no better element than a log that can give details about the attack, which allows the organization to act on it. Logs play a bigger role than they used to. They are not simply used for troubleshooting anymore, they have become important for network and system performance optimization, tracking user actions, providing data for investigating suspicious activity. In many cases, having log data easily available can provide early warnings about problems before they spiral out of control. These largely produced data will provide the organization a better insight into their own infrastructure, hence centralized logging can be very useful when attempting to identify problems with the servers or applications, as it allows searching through all of the logs in a single place. It is also useful because it allows identifying issues that cause troubleshooting for multiple servers by correlating their logs during a specific time frame. The volume of data generated from the systems events is of considerable importance as a source of information for any organization. The proper control of this data ensures that the legal compliance obligations will be accomplished and to address IT security risk. The need to include the real-time monitoring of the network arises from the growing threats to business continuity. Businesses need to be able to make a thorough analysis and detailed report-data to meet stringent

and ever more demanding legal and compliance obligations. It is of crucial importance for an IT department of any organization to be able to efficiently track any event in the network within a needed time frame. One logical solution to this issue is to send all logs into a central log server. Modern log protocols support encryption and authentication to secure the log collection. Software developments, website administration, network administration, incident response are some example activities that require efficient log management.

III. PROPOSED LOG-BASED STRATEGY

In order to collect logs and have them presented in a comprehensive format, it is very important to make an intensive research before choosing the appropriate tool for log management. In order to meet regulatory compliance standards, all logs must be collected—not just the security logs. For example, operating system logs and application logs often contain security-related information as well as information about events that may not initially appear security related. Organizations must consider the potential value of every possible log source. Organizations who are using cloud services, should have at least a minimum grasp of their infrastructure, and be alarmed and proactive to deal with attacks or malfunctions of their system. Instead of having the logs analyzed inside the cloud it would be more efficient to integrate the log management solution chosen by the organization and let them have total control over it. Before the organization starts monitoring their data by analyzing the logs, an approach should be taken to assure the security of the data. The approach comes in three steps(figure 1 and table 1).

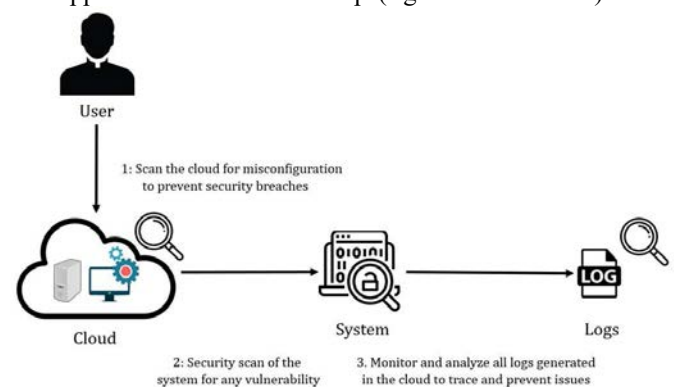


Figure 1. Three step Log-based Proactive Strategy

The first step to do in the cloud should be, is to set a solution that would do a complete security scan to the cloud to detect any misconfiguration or security breach. Basically, the constant analysis of the cloud configuration can detect whether an attack happened or is in progress. The security scanning of the cloud configuration is very important.

The second step to follow is to integrate a vulnerability scanning tool analysis. With security attacks are on the rise for cloud computing, the system needs to be properly tested for any vulnerabilities and security needs to be secured.

The third step is to monitor and analyze the logs generated in the cloud using a log management solution that provides real-time analysis and alerts triggering functions to better manage the system.

A. Cloud configuration checking

As the cloud is under constant threat of being attacked every second, it is essential to make sure its configuration and the services used in the cloud are always under consistent and up-to-date configuration, because misconfiguration can compromise the cloud and its components by exposing its assets and by making it a target for cyber-attacks. In a Coalfire published report, a survey conducted about the cloud's security concerns[9], misconfiguration of the cloud was the concern of 40 percent of the respondents.

The first step to do in the cloud should be to set a solution that would do a complete security scan to the cloud to detect any misconfiguration or security breach. Constant analysis of the cloud configuration can detect whether an attack happened or in progress because the IT administrator would be able to detect if the configuration has been changed. Security scanning of the cloud configuration is very important. For example, it can happen that one of the developers opens a data store when developing a part of the software and leaves it open when releasing the application to the market, and that can cause a real security breach. Numerous tools that can be used to detect misconfiguration in the cloud, such as:

- Checkov[6]: Python-based software to scan cloud infrastructure.
- Terraform[7]: a tool that scans cloud IaC to detect any misconfiguration.
- CloudSploit[8]: an open-source project that can detect misconfiguration. CloudSploit scans the code for any misconfiguration.

Figure 2 shows a basic process of misconfiguration detection.

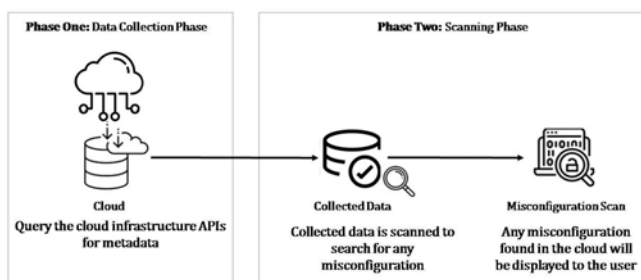


Figure 2. Misconfiguration scanning architecture

B. Vulnerability scanning

Most of the common security breaches in the cloud are basically unauthorized access. Cloud's complicated infrastructure can cause a lot of vulnerabilities, so it is very important to ensure detection of the cloud's vulnerabilities. In a survey targeting organizations' concerns about cloud security, published by Coalfire[9], 93 percent of enterprises

and organizations were extremely concerned about cloud security. With the cloud being constantly under threat of being attacked and compromised, the attacker can use the cloud's vulnerability as a loophole to lead a successful attack on the cloud. Vulnerabilities that an attacker can make use of are numerous such as:

- Data breaches: The release of private information intentionally or unintentionally publically.
- Malware and ransomware: attackers infect and encrypt files until the user pays the ransom to free the data use malware.
- Denial of service(DoS) and distributed denial of service(DDoS): DoS tries to make resources unavailable to its users by flooding the target. DoS uses one source and DDoS uses more than one source at the same time.
- Data Loss: Data loss in the cloud can happen due to a lot of factors. One of them can be hardware limited storage.
- Insecure API: As APIs in the cloud is not secure, they have become an easy target for attackers to use in their attack in the cloud.
- Vendor Lockin: When an organization uses a cloud provider, they are dependent on a single cloud provider which makes it hard to change vendors.

As organizations still do not fully understand the different aspects of their cloud's security, with vulnerability issues remaining as one of the top concerns making organizations reluctant towards using the cloud, it became a necessity for organizations to understand that the security of the cloud is a shared responsibility between the cloud's service provider and the organization. The organization should not rely on the cloud provider for security scan because cloud security is a shared responsibility. As emphasized in this paper, scanning for cloud vulnerability is a focal point.

The second step to follow is to integrate a vulnerability scanning tool. Most cloud services such as IBM and Google are sure revolutionary, however, security issues still remain. With security attacks are on the rise for cloud computing, they need to be properly test for any vulnerabilities and ensure the security. Choosing the right vulnerability scanner is important, and there are a lot of open-source/paid vulnerability scanners, to name a few:

- NMAP[10]: Nmap is a tool used for scanning net-works, however, Nmap supports only a few OS like Unix, Linux, Solaris, Mac, windows, and other operating systems.
- Nexpose[11]: Nexpose is an open-source tool used for scanning for vulnerabilities. Its database is constantly updated by new vulnerabilities by the github community weekly.
- Arachni[12]: Arachni is a scanner ruby based used for web applications. Arachni can detect vulnerabilities like Cross-site request forgery, Code injections. The process Arachni uses for vulnerability detection is in figure 3.
- Nikto[13]: Nikto is capable of testing against 6700 dangerous risks. It is available in kali linux.

- sqlmap[14]: sqlmap is an open-source testing tool that automates detection of vulnerabilities. This tool can be adapted to any operating system since the tool is developed in Python.
- Wapiti[15]: Wapiti is an application that uses command lines to test web applications for vulnerabilities.

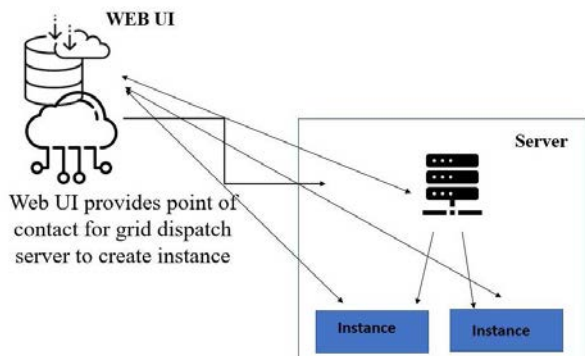


Figure 3. Vulnerability scan tool basic architecture "Arachni as an example"

C. Log management

Logs should be collected and transformed into a more comprehensive format to make it easier to manage. Because choosing the right tool to manage logs is not an easy task, intensive research must be done before choosing the appropriate tool to manage the logs. All different kinds of logs must be collected to be able to have a thorough analysis, and the search for the appropriate tool should be done according to the requirement of the organization.

Centralized logging can be very useful when attempting to identify problems with the servers or applications, as it allows search through all of the logs in a single place. It is also useful because it allows identifying issues that cause troubleshooting for multiple servers by correlating their logs during a specific time frame. The volume of data generated by the systems events is of considerable importance as a source of information for any organization. The proper control of this data ensures that the legal & compliance obligations can be accomplished and IT security risk to be addressed. The need to include the real-time monitoring of the network arises from the growing threats to business continuity. It is of crucial importance for an IT department of any organization to be able to efficiently track any event in the network within a needed time frame. One logical solution to this issue is to send all logs into a central log server. Modern log protocols support encryption and authentication to secure the log collection. Software developments, website administration, network administration, incident response are some examples of activities that require efficient log management.

The third step to follow through is to monitor and analyze the logs generated in the cloud using a log management solution that provides real-time analysis, and to alert triggering functions to better manage the system.

	Goal	Role
Step one	Avoid any major security breaches (e.g. release of sensitive information)	Detection of any misconfiguration in the cloud, in order to guarantee the integrity of the system
Step two	Secure cloud against any upcoming threats	Detection of any vulnerabilities that can be used by attackers as loopholes
Step three	Better manage the system's data	Centralized logging helps taking a proactive approach to security and troubleshooting

Table 1. Different steps to take as security measures

Organizations must consider the potential value of every possible log source. There are a lot of types of logs that are being generated in the system, and here are some log types that must be considered for log collection to ensure efficiency:

- Anti-Malware software: Examples of anti-malware include anti-virus and anti-spyware. These logs may include information like indicators that malware was detected, disinfection attempt results, file quarantines when file-system scans were last performed.
- Applications: The information logged by applications can vary widely and may include account changes, user authentication attempts, use of privileges, usage details, client and server activity, configuration changes, major system failures, and more.
- Authentication servers: Directory servers and single sign-on servers will typically log every authentication attempt showing the originating user ID, destination system or application, date and time information, and success/failure details.
- Firewalls: Firewalls can inspect content and ensure the state and integrity of permitted connections.
- Network devices: Routers can be configured to block certain types of traffic. Network devices can be configured to log detailed connection activity, but it is usually configured to log lightly. The produced can contain very informative network communication activity.
- Operating systems: There are many varied operating systems on servers, workstations, and assorted network devices. The host administrator typically controls logging. The types of events, as well as whether to log only successful or only failed events, or both, can be controlled. These log entries typically contain information about service starts and stops, authentication attempts, file accesses, account changes, permission and privilege changes, and use of privileges.
- Vulnerability management software: Included here are both vulnerability scanning and patch management software. These typically run on an occasional basis and log batches of log entries that include information about scanned hosts/devices including: configuration, missing software updates, vulnerabilities identified, and patch/scan currency downloads, among other things.

There are a lot of log management solutions to choose from so it is important to make the right choice. The log management tool that is needed must be capable to:

- filter real-time logs

- help treat pre-configured exceptions
- powerfully search syntax
- drill-down analysis: field statistics, quick values
- alert and trigger: get notified when something needs attention, such as failed login attempts, exceptions or performance degradation.
- give all users secure access to real-time data.
- rest API
- output: forward data to specialized systems or anything else that needs a real-time stream of data.

The basic overview of the existing and most efficient log management solutions are presented in Table 2. The presented solutions require configuration, so the user must be aware of their own infrastructure.

Program	Logstash	Kibana		GrayLog2	Fluentd
		Kibana3	Kibana 4		
Language	Java/Ruby	Javascript	Javascript	Java/Ruby	Ruby
License	Apache 2.0	Apache 2.0	Apache 2.0	GPLv3	Apache 2.0
Protocol	BSD Syslog UDP,IETF syslog UDP,IETF TCP,Gelf	BSD & IETF syslog, AMQP, XMPP...		BSD & IETF syslog, GELF, GELF via Http AMQP	HTTP,AMQP,OMQ Kafka
Storage	Elasticsearch	Elasticsearch		Elasticsearch, MongoDB	Elasticsearch
Indexing	Elasticsearch	Elasticsearch		Elasticsearch	Elasticsearch
Transport	TCP,UDP	TCP,UDP		TCP,UDP	TCP,UDP

Table 2. Basic overview of existing log management solutions

IV. CONCLUSIONS

The recent rise of attacks on clouds has been a major problem for companies and organizations. These attacks have resulted in mistrust between cloud providers and their consumers. Companies and organizations should be well informed of their provided cloud infrastructure and how to secure it. This paper aims to help companies and organizations manage their own resources by highlighting the current security challenges. Cloud computing is experiencing and proposing a strategy with appropriate measures that should be adopted for an organization or a company to understand the security threats their cloud is facing. We propose a three-step strategy to take to better secure the cloud. Firstly, it is important to make sure the cloud is not facing any misconfiguration. Misconfiguration of the cloud can cause a huge security breach. Setting solutions that would do a complete security scan to the cloud is very important to detect any misconfiguration or security breach. Any cloud can have vulnerabilities and these vulnerabilities can be used by attackers as a loophole for their attacks. The second step to follow is to integrate a vulnerability scanning tool analysis. Nowadays system logs play a major role in preventing attacks and securing any system. Therefore, centralization of the cloud log is very important as it can help identify problems and be used for troubleshooting. The third step to follow through is to monitor and analyze logs generated in the cloud using a log management solution that provides real-time analysis, and to alert triggering functions to better manage the

system. In future work, we will implement our proposed strategy and analyse it in a scenario to test how secure it can be against attacks and existing threats on the cloud.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2020R1A2C1006497). Inshil Doh is the corresponding author.

REFERENCES

- [1] "Centralized Logging Solutions," <https://labs.elecs.com/2014/05/centralized-logging-solutions-overview.html/>
- [2] McAfee, "Cloud adoption and risk report: Work from home edition," 2020.
- [3] R.Boutaba,L.Cheng,Q.Zhang, "On Cloud computational models and the heterogeneity challenge," Journal of Internet Services and Applications, 2011
- [4] A.Balobaid,W.Alawad and H.Aljasim, "A Study on the Impacts of DoS and DDoS Attacks on Cloud and Mitigation Techniques International Conference on Computing," Analytics and Security Trends, 2016
- [5] A.Alshammari, S.Alhaidari, A.Alharbi and M.Zohdy, "Security Threats and Challenges in Cloud Computing," in Magnetism, vol. III, IEEE 4th International Conference on Cyber Security and Cloud Computing 2017.
- [6] "Checkov by bridgecrew," <https://github.com/bridgecrewio/checkov>
- [7] "Terraforma," <https://github.com/wayfair/terraforma>
- [8] "CloudSploit by Aqua," <https://github.com/aquasecurity/cloudsploit>
- [9] C. Coalfire, "Cloud security intelligence report," <https://www.coalfire.com/documents/whitepapers/securealities-cloudsecurity-report>, 2019.
- [10] "NMAP," <https://nmap.org/>
- [11] "Nexpose," <https://www.rapid7.com/products/nexpose/>
- [12] "Arachni," <https://github.com/Arachni/arachni>
- [13] "Nikto," <https://github.com/sullo/nikto>
- [14] "sqlmap," <https://github.com/sqlmapproject/sqlmap>
- [15] "wapiti," <https://wapiti.sourceforge.io/>



Oumayma Mejri is a Tunisian citizen. In 2016, Oumayma Mejri has obtained a bachelor degree in Tunisia majoring in Network and services managements from the Higher institute of computer science Tunis Al manar, Tunisia. During the last year at university, she had 4 month internship at Tunisia's leading company in telecommunications, and has finished her internship with a thesis to help the company set up a log management solution. After graduation, she has focused on volunteer work and gaining experience in different fields by doing different internships. In 2018, she obtained a scholarship from the Korean Government for a master's degree in cyber security at Ewha Womans University along with a yearlong Korean language course at Chosun university in Gwangju.



Dana Yang received the B.S. degree in the Department of computer software at Korean Bible University in 2013. She is currently a Ph.D. candidate in the Department of computer science and engineering at Ewha Womans University, Seoul, Korea. Her research interests include authentication, blockchain, steganography, FANET (Flying Adhoc

Network) security, and D2D network security. She also received the outstanding paper award in the 20th International Conference on Advanced Communication Technology (ICACTION) in 2018.



Inshil Doh received her B.S. and M.S. in Computer Science and Engineering at Ewha Womans University, Korea, in 1993 and 1995, respectively. She received her Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995 to 1998, She worked at Samsung SDS of Korea. She was a research professor at Ewha Womans University in 2009, 2010, and at Sungkyunkwan University in 2011. She is currently an associate professor of the Department of Cyber Security at Ewha Womans

University, Seoul, Korea. Her research interests include data communication security and privacy, sensor network security, and IoT network security.