Internet of Things and Cloud Computing
2022; 10(3): 33-36
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20221003.11
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

Cyber Security Architecture Components for Cloud Network

Thierry Mbah Mbelli

Assupol Life, Pretoria, South Africa

Email address:
thierrym@assupol.co.za

To cite this article:
Thierry Mbah Mbelli. Cyber Security Architecture Components for Cloud Network. *Internet of Things and Cloud Computing*. Vol. 10, No. 3, 2022, pp. 33-36. doi: 10.11648/j.iotcc.20221003.11

Received: August 8, 2022; **Accepted**: August 29, 2022; **Published**: November 30, 2022

Abstract: The cyber security landscape is constantly evolving and changing with attackers developing new tools and techniques to access organizations' systems and data. Public and private organizations are finding it increasingly difficult to defend their systems and data from these constantly changing, evolving, and persistent threats. Therefore, it is empirical and critical that both business and government agencies protect their systems and data from potential risks arising from these threats for business or organization continuity. Cybercriminals often target the networks to launch attacks on the organization-targeted systems with the intention to gain access and either steal, alter or destroy value data. These attacks may include Malware, DDoS, SQL injection, Phishing, XSS, Botnets, and many more. Cloud adoption has fundamentally changed the way applications are delivered and consumed. Traditional networks lack the security and performance capabilities and therefore cannot support these new cloud challenges. This paper proposes an architecture with built-in algorithms to detect both new and old threats. The paper starts with an analysis of the challenges for intelligent networks. The second part looks at related works that have been carried out in relation to cybersecurity in networks. The third part proposes an architecture with an algorithm built in to detect new threats to the networks. Finally, the last part deals with the implementation of the architecture.

Keywords: Cloud Networks, Cloud Services, Cyber-Attacks, Traditional Networks, Cyber Security, Big Data, Machine Learning

1. Introduction

Organizations are turning to cloud-based solutions to meet their business and technology needs. Cloud services and applications offer tremendous benefits in terms of cost reduction compared to on-premises services and applications. These benefits come in the form of higher performance, flexibility, and scalability. But with all these benefits come increased security risk and high demands on cloud networks. Wide-Area Network (WAN) plays a critical role in connecting cloud users and devices to the cloud infrastructure. The challenges faced by WAN are the inability to work optimally, reliably and securely. Therefore, an intelligent method to monitor and detect threats to cloud network is needed.

Despite innovations in protecting cloud networks, cyber attackers' methods are becoming more sophisticated and changing. Cyber attackers often use powerful artificial intelligence mechanisms to penetrate networks and gain access to organizations systems and data. With advanced tools at their disposal, they can execute and install malware in real time. This is a real challenge, especially in an environment that contains a huge amount of data. Attack patterns change often, and in order to catch up and outsmart the attackers, a data-driven option is a great opportunity. Cyber attackers take control when cloud users access resources on the cloud networks through intranet or internet by intercepting the connection.

This paper addresses the development of a robust algorithm-driven architecture that can monitor the cloud network with big data analytics and machine learning capabilities to detect suspicious threats in the network and take proactive measures to avert attacks. The rest of this article is structured as follows: Section II discusses the related work that has been done in securing cloud networks. Section III discusses the security challenges faced by cloud networks. Section IV gives an overview of the proposed architecture of cyber security cloud networks to detect threats in networks. Section V discusses the implementation of the architecture. Finally, Section VI concludes the paper.

2. Related Work

R. Savold, N. Dagher, P. Frazier and D. McCallam [1] discussed how an attacker can intrude a network connection and take control of user's resources that are hosted on cloud networks. The paper proposed a combined approach of signature and proactive based approaches to negate attacks based on signature detection modules. The proactive approach proposed by R. Savold, N. Dagher, P. Frazier and D. McCallam [1] also add detection capabilities by incorporating honeypot-based solution in the cloud networks.

One of the major challenges that organizations face is to choose among the hundreds or thousands of available cyber security products and at the same time maximizing their investments to protect against new and old threats. R. Savold, N. Dagher, P. Frazier and D. McCallam [4] discussed the role of reference architectures in designing cyber security architectures. The paper also discussed the different models that are currently being used in recent cyber security architecture ecosystem.

In L. Wang and R. Jones [8] the variety and veracity of big data characteristics in network traffic and attacks are looked at, where two types of datasets were used. One of the datasets focused on numeric and symbolic data and the other focused on missing values. The correlation coefficient of the variables, cluster and duplicate analysis are done on one of the datasets and data quality analysis is done on the other dataset.

A. Bilen and A. B. Özer [15] analyzed cyber-crimes using two different models that incorporated machine learning methods to predict the effect of defined features on detection of an attack. In this study, eight machine learning methods were used with the support vector machine linear found as the most successful with an accuracy rate of more than 95 percent. The logistic regression method was found to be the leading method in detecting attackers with an accuracy rate of more than 65 percent.

A. Giehl and S. Plaga [2] proposed an architecture with two deployment modes (in-line and out-of-band) with in-line mode having security functions that need to act in real time and deployed together with network traffic while the out-of-band mode is mainly used for monitoring the network traffic and generating alarms.

3. Cloud Network Security Challenges

The cloud platforms are becoming the platforms of choice for many businesses today because of the financial benefits they bring and with this vibe, the cyber criminals are targeting the cloud networks. Most organizations pay more attention to cloud services and applications that are on offer with little attention to the networking aspect of the cloud ecosystem. For cloud services and applications to run optimally, they need a flexible and secure network.

Network-based attacks and intrusion detection are detected based on unusual behavior patterns that look at the use of networks with high-speed big data interfaces D. S. Terzi and R. Terzi, S. Sagiroglu [9].

With increasing number of IoT-based devices and interconnectivity between them that share sensitive personal data pose a huge security challenge which could be an easy target for attacks by cyber hackers. These potential attacks can be caused by vulnerabilities in IoT devices which hackers can consider and exploit as an entry point to crack victims' sensitive and secure infrastructures S. Sen and C. Jayawardena [7]. There are difficulties in separating the IoT framework information from individual information and the security of what big information uses C. B. M. Reddy, U. k. Reddy, E. Brumancia, R. M. Gomathi and K. Indira [11].

The following describes some of the security challenges in cloud networks.

1. Auto scaling serverless computing might cause vulnerability scanning difficult because vulnerable assets might have very short lifespan and this can give the cyber criminals enough time to find and exploit.
2. Cloud infrastructure is simple and easy to setup by any person with the right credentials and this makes it easier to expand the cloud network which might not be configured securely and thus open for attack.
3. The hybrid architecture of some cloud networks makes it a security challenge since information is stored in different systems and needs to be protected using different security tools.
4. Cloud network security challenges can occur at the network level that deals with network protocols, user authentication level that deals with encryption and authentication methods, data level that deals with data integrity and generic level that deals with the usage of different security tools M. B. Sridhar and A. Koushik [3].

4. Cyber Security Architecture

The goal of the architecture is to detect new and old (internal and external) threats by understand the threat sources. Various algorithms and tools have been developed to combat cyber threats. As more sophisticated tools and techniques are developed by the cyber criminals, there is need to develop accurate defense techniques to guard against these. Machine learning is one of these techniques that can be utilized to detect infectious activities and policy violations in a network B. Arpitha, R. Sharan, B. Brunda, D. Indrakumar and B. E. Ramesh [16].

This architecture is based on big data integrated with machine learning to automate the process of identifying patterns and predicting and mitigating potential cyber-attacks by providing a machine learning algorithm to bring predictive network security. This algorithm is based on deep learning techniques. Deep learning constructs artificial neural networks thus simulating the interconnection of neurons of human brains which provides the power to solve very complicated problem Y. Wu, D. Wei and J. Feng [13].

Cyber-attacks can be traced to the IP address space using attack pattern which describes the frequency of attacks per IP address B. Gokaraju, R. Agrawal, D. A. Doss ans S. Bhattacharya [6].

This architecture uses network behavior anomaly detection to detect known and unknown attacks or threats in the network. The network behavior anomaly detection can detect many different types of anomalies and threats. Such anomalies and threats can include payload, IP and MAC spoofing, virus, bandwidth and connection rate Y. S. K. Vani, Krishnamurthy [12].

The architecture design uses top-down approach, starting with high-level abstraction and ending with technology binding. Low-level architecture elements are automatically extracted G. Buchgeher and R. Weinreich [18].

The main components of the architecture as shown in figure 1:

1. Machine /Deep Learning (ML/DL) module – the main analytics engine using proposed algorithm. This module has the artificial intelligence (AI) and data analytics subcomponents. The AI applies the algorithm while the data analytics fetch data from configuration and reference data components.
2. DNS registry – the ML/DL checks the IP addresses and domain names in the DNS registry.
3. Config/Reference data – the ML/DL checks these data sources if threat exists, if the threat doesn't exit it will add it to the data source.
4. Notification/Alarm – this component is used to send notifications and information on the action that was taken.
5. The proposed algorithm is the Random Vector Regression RVR which has the capability of randomly mapping non-linear data points into a different linearly separable dimension. The RVR has a high ability to classify data points accurately.

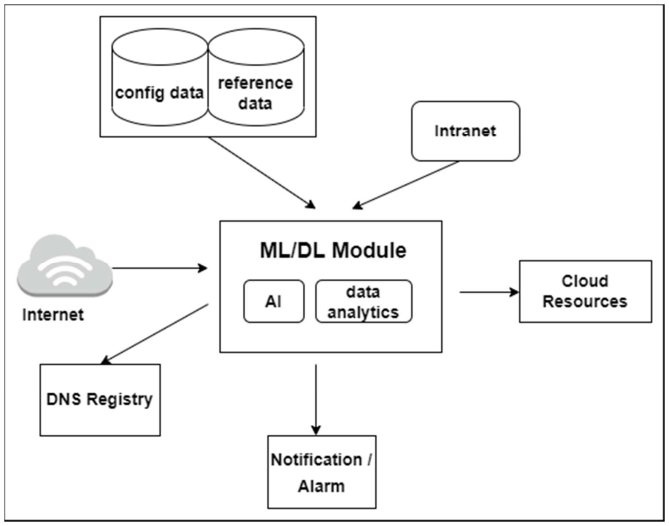

Figure 1. *Cyber security architecture.*

5. Technical Implementation

To successfully analyze and detect possible threats, a modelling approach is highly recommended. The STRIDE which is a lightweight threat modeling framework analyzes threats using six categories; user identity spoofing, DoS, message tampering, disclosure and privilege A. Giehl and S. Plaga [5].

In the machine / deep learning module, heuristics and aggregation domains will be applied through clustering and using artificial intelligence.

Machine learning and deep learning greatly increase the calculation probability of detecting anomalies and threats based on statistical methods and big data by making computers camouflage human way of thinking M. Aljabri, S. S. Aljameel, R. M. A. Mohammad, S. H. Almotiri, S. Mirza, F. M. Anis, M. Aboulnour, D. M. Alomari, D. H. Alhamed and H. S. Altamimi [14]. The machine learning and deep learning module is been fed with network data that is used to train the algorithm to detect traffic as normal, abnormal or malicious. Once the algorithm detects a malicious traffic, it triggers appropriate action(s) to prevent the intrusion or attack.

The proposed algorithm to be used in this architecture is the Random Vector Regression RVR which has the capability of randomly mapping non-linear data points into a different linearly separable dimension. The RVR is a combination of support vector regression and random forest techniques which has a high ability to classify data points accurately.

A decision tree or random forest which is an algorithm that has several decision trees with different samples and features that are randomly sampled. These can be used to detect anomaly in a network C. Zhang, X. Shen, X. Pei and Y. Yao [10]. An algorithm selection is based on three stages namely; analytical objective, analytical approach and analytical technique M. Chalé, N. D. Bastian and J. Weir [17].

The machine /deep learning module will read all the IPs related information from the DNS registry to classify source and targeted systems using ICANN lookup.

6. Conclusion

Cloud Network enables organizations to efficiently connect users to the cloud and host its IT infrastructure capabilities and resources in a private or public cloud platform. The security of these networks is still a concern as attackers are continually optimizing their attack mechanisms. This paper looks at the challenges faced by cloud networks in terms of security and proposes an architecture to analyze and detect anomalies and threats on cloud mainly using supervised methods. Big Data Analytics and artificial intelligence used in the architecture facilitate better detection of threats and attacks, management of potential risks, intercepting and monitoring of possible attacks or threats, automating of response and taking action. Machine learning algorithms help with analysis of current and future threat patterns and offering real-time predictions. The architecture takes into consideration the current threat patterns and formulation of future patterns.

References

[1] S. Puri, M. Agnihotri, "A Proactive approach for cyber attack mitigation in cloud network," International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017.

[2] A. Shameli-Sendi, Y. Jarraya, M. Pourzandi, M. Cheriet, "Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns" IEEE Transactions on Services Computing, 2019, vol. 12, issue 4.

[3] M. B. Sridhar, A. Koushik, "A Study of Big Data Analytics in Clouds with a Security Perspective," International Journal of Engineering Research & Technology (IJERT), 2017, vol. 6, issue 1.

[4] R. Savold, N. Dagher, P. Frazier, D. McCallam, "Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks," IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017.

[5] A. Giehl, S. Plaga, "Implementing a performant security control for Industrial Ethernet," International Conference on Signal Processing and Information Security (ICSPIS), 2018.

[6] B. Gokaraju, R. Agrawal, D. A. Doss, S. Bhattacharya, "Identification of Spatio-Temporal Patterns in Cyber Security for Detecting the Signature Identity of Hacker," SoutheastCon, 2018.

[7] S. Sen, C. Jayawardena, "Analysis of Cyber-Attack in Big Data IoT and Cyber-Physical Systems - A Technical Approach to Cybersecurity Modeling," IEEE 5th International Conference for Convergence in Technology (I2CT), 2019.

[8] L. Wang, R. Jones, "Big Data Analytics of Network Traffic and Attacks," IEEE National Aerospace and Electronics Conference (NAECON), 2018.

[9] D. S. Terzi, R. Terzi, S. Sagiroglu, "Big data analytics for network anomaly detection from netflow data," International Conference on Computer Science and Engineering (UBMK), 2017.

[10] C. Zhang, X. Shen, X. Pei, Y. Yao, "Applying Big Data Analytics Into Network Security: Challenges, Techniques and Outlooks," IEEE International Conference on Smart Cloud (Smart Cloud), 2016.

[11] C. B. M. Reddy, U. k. Reddy, E. Brumancia, R. M. Gomathi, K. Indira, "Integrative Approach Of Big Data And Network Attacks Analysis In Cloud Environment," 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020.

[12] Y. S. K. Vani, Krishnamurthy, "Survey anomaly detection in network using big data analytics," International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017.

[13] Y. Wu, D. Wei, J. Feng, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey," Security and Communication Networks, Vol. 2020.

[14] M. Aljabri, S. S. Aljameel, R. M. A. Mohammad, S. H. Almotiri, S. Mirza, F. M. Anis, M. Aboulnour, D. M. Alomari, D. H. Alhamed, H. S. Altamimi, "Intelligent Techniques for Detecting Network Attacks: Review and Research Directions," Sensors 2021.

[15] A. Bilen, A. B. Özer, "Cyber-attack method and perpetrator prediction using machine learning algorithms," PeerJ Computer Science, April 2021.

[16] B. Arpitha, R. Sharan, B. Brunda, D. Indrakumar, B. E. Ramesh, "Cyber Attack Detection and notifying system using ML Techniques," IJESC, 2021. Vol. 11. Issue No. 06.

[17] M. Chalé, N. D. Bastian, J. Weir, "Algorithm Selection Framework for Cyber Attack Detection," WiseML, 2020.

[18] G. Buchgeher, R. Weinreich, "Connecting Architecture and Implementation," Proceedings of the Confederated International Workshops and Posters on On the Move to Meaningful Internet Systems, 2009.