AIRO JOURNALS

Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume: 2 Issue:3
June 2022
Impact Factor:5.7
Subject: Computer Science

MANAGEMENT OF SECURITY IN A COMPUTER NETWORK FROM BOTH INTERNAL AND EXTERNAL THREATS

Rounak R. Gupta
Research Scholar, University of Technology, Jaipur
Dr. Pramod Sharma
Professor, University of Technology, Jaipur
rounak_gupta@rediffmail.com

DECLARATION: I AS AN AUTHOR OF THIS PAPER / ARTICLE, HEREBY DECLARE THAT THE PAPER SUBMITTED BY ME FOR PUBLICATION IN THE JOURNAL IS COMPLETELY MY OWN GENUINE PAPER. IF ANYISSUE REGARDING COPYRIGHT/PATENT/ OTHER REAL AUTHOR ARISES, THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENT AMENDMENT/ OR ANY TECHNICAL ISSUE WITH NO VISIBILITY ON WEBSITE/UPDATES, I HAVE RESUBMITTED THIS PAPER FOR THE PUBLICATION. FOR ANY PUBLICATION MATTERS OR ANY INFORMATION INTENTIONALLY HIDDEN BY ME OR OTHERWISE, I SHALL BE LEGALLY RESPONSIBLE. (COMPLETE DECLARATION OF THE AUTHOR AT THE LASTPAGE OF THIS PAPER/ARTICLE)

Abstract:

Recent years have seen a meteoric rise in the amount of internet traffic coming from social media websites. This may be attributed to the continued creation and utilization of applications and services based on multimedia content. As a result of the broad expansion and interest in utilizing social method online portals all over the world, network-based communications are becoming increasingly susceptible to a variety of security risks known as anomalies in the modern day. Therefore, it is required to scan the multimedia communications that take place inside Online Social Networking (OSN) in order to identify any potential security issues that may endanger the important data of end users. Finding out all of the requirements for OSNs, such as Quality of Service (QoS), dependability, and measurability plays a key role in the process of designing a paradigm for the safe transmission of multimedia data.

Keywords: Online, social, Networking, websites, quality, service, etc.

1. INTRODUCTION

The growth of the Internet from a network of things to a network of thoughts has contributed to the rise in popularity of social networking. It is the broadest, richest, and most dynamic evidence base of human behavior, which brings about new potential for a better understanding of people, communities, and civilizations. Recent research conducted in the field of social media suggests that around 4 billion people are using the internet at this moment all over the world, with more than 3 billion of those people actively using social media. Multimedia content is expanding at a rate that has never been seen before as a direct result of the expansion of social networks. Despite this, significant insights might be difficult to glean from this thriving and ever-expanding body of data due to the content-driven and object-oriented nature of social multimedia. In addition, the extensive multimedia content that is made available on social networks contains information that is sensitive and private regarding people and the interactions that they have with one another. Because there is such a large quantity of freely available personal information, it is extremely susceptible to attacks, the majority of which end in the theft of information and identity. Therefore, interoperability and security are the two most significant difficulties in the architecture that lies under the surface. For this reason, a communication paradigm that is both scalable and pervasive is necessary for data analytics and the administration of social multi-media data while yet preserving an appropriate level of safety. In recent years, researchers in the field of cyber security have developed a great number of anomaly detection models in order to protect the network from attacks that are carried out by malicious users against a variety of multimedia applications. Some of these applications include videoconferencing, real-time content delivery, online gaming, and remote video-on-demand. Deep learning architectures, such as Convolutional Neural Networks (CNN), Deep Belief Networks (DBN), Restricted Boltzmann Machines (RBM), Stacked Auto Encoders, Recurrent Neural Networks (RNN), etc., are utilized extensively in this approach. For instance, abnormal event detection schemes for videos, in which they used three-dimensional CNN to extract the spatiotemporal information of the inputs; a method for the detection of unusual events in videos via stacked sparse coding and intra-frame classification strategies based on the probabilistic outputs of SVM; and a fully CNN to detect anomalies in crowded activities. All of these are examples. Another example would be a full CNN to detect anomalies in crowded activities. In comparison to the conventional techniques of machine learning, these methods are significantly more popular in the field of pattern recognition due to the fact that they are founded on end-to-end training and representation learning. The training of deep learning methods is computationally expensive and needs a vast amount of data; nevertheless, the coupling of these methods with reinforcement learning might be effective.

2. SOFTWARE-DEFINED NETWORKING (SDN)

Software-Defined Networking, often known as SDN, is a method of networking that communicates with the underlying hardware architecture of a network through the use of software-based controllers or application programming interfaces (APIs). This method is used to route traffic through a network. This paradigm is distinct from the one utilized by conventional networks, which make use of specialized pieces of hardware (i.e., routers and switches) to regulate the flow of data throughout the network. Software-defined networking is capable of creating and controlling a virtual network as well as controlling conventional hardware. Software-defined networking enables a new method of controlling the routing of data packets through a centralized server. Network virtualization enables organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network. Software-defined networking also enables organizations to connect devices on different physical networks to create a single virtual network. The purpose of applications is dynamically interpreted by the SDN controller, which then injects rules into switches that are capable of SDN. The inspection, modification, and forwarding of packets are carried out by the SDN switches in accordance with these principles. They have the ability to inspect and edit the packet headers at various levels of the protocol stack, from the data link layer up to the application layer. Through the use of a centralized controller, Software-Defined Networking (SDN) intends to facilitate the speedy reaction of network managers to shifting topology, traffic, or business requirements. In the course of our work, we implement SDN in the backbone networks that are responsible for the transmission of packet flows to make the interchange of data between SCADA systems more dependable and adaptable. SDN makes it much simpler to adjust to new circumstances, and it also makes it possible to achieve both a low rate of packet loss and flexible packet forwarding.

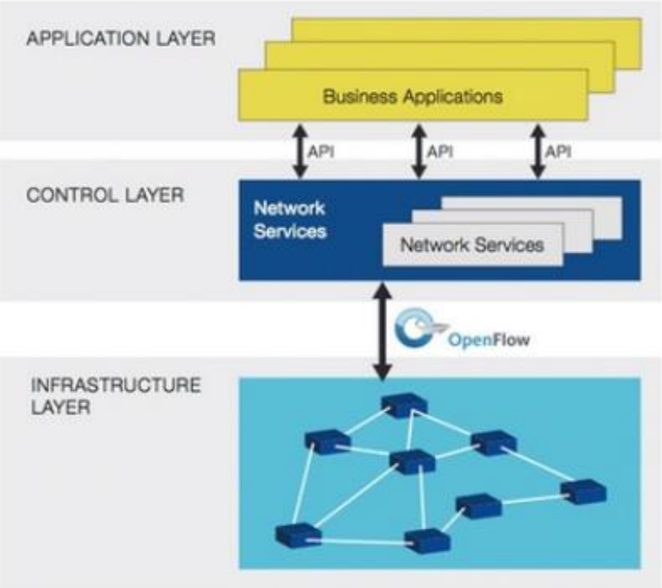

Figure 1: Framework of SDN

3. THE COMPONENTS OF SOFTWARE-DEFINED NETWORKING

The acronym SDN refers to software-defined networking, which is comprised of three primary components, any two of which may or may not be physically situated in the same location:

- Applications that either transmit information about the network or make queries regarding the availability or distribution of specified resources.

- SDN controllers are responsible for determining the destination of data packets by communicating with the applications. Within SDN, the load balancers are referred to as the controllers.

- Networking devices that are instructed on how to route packets by the controllers. These devices receive such instructions from the controllers.

In addition to these components, software-defined networking (SDN) also makes use of Open Flow, which is a programmable networking protocol that moves traffic among network devices. Standardization of the Open Flow protocol and other open source software-defined networking technologies was assisted by the Open Networking Foundation (ONF). These components come together to form SDN ecosystems, which are responsible for ensuring the correct flow of network traffic.

4. ANOMALY DETECTION

Finding patterns in data that do not conform to the behavior that is anticipated is the challenge that is referred to as anomaly detection. In various application fields, these non-conforming patterns are frequently referred to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, quirks, or contaminants. These are all names for the same type of pattern. Anomalies and outliers are two words that are used most frequently in the context of anomaly identification; in fact, they are sometimes considered to be interchangeable with one another. A large number of different

ISSN: 2320-3714
Volume: 2 Issue:3
June 2022
Impact Factor: 5.7
Subject: Computer Science

applications make considerable use of anomaly detection, including fraud detection for credit cards, insurance, and health care; intrusion detection for cyber security; failure detection in safety essential equipment; and military surveillance for enemy operations. Anomalies in data may translate to substantial (and frequently essential) actionable information in a broad number of application areas, which is one of the reasons why anomaly detection is considered to be so important. For instance, an unusual traffic pattern in a computer network might be an indication that a machine that has been hacked is transmitting sensitive data to a location that is not allowed to receive it. An unusual appearance on an MRI scan might point to the existence of cancerous tumors. An anomaly in the data of a credit card transaction might indicate that the card was stolen, as could an anomaly in the readings of a sensor on a spacecraft, which could indicate that there is a problem with one of the spacecraft's components. Since the 19th century, researchers in the field of statistics have been trying to figure out how to identify outliers and other irregularities in data. Over the course of time, several research communities have come up with a range of different strategies for the identification of anomalies. While several of these methods have been created expressly for certain application fields, others are more general. This survey makes an effort to present a logical and all-encompassing summary of the research on anomaly detection. We have high hopes that it will help people gain a better understanding of the many different ways that research has been conducted on this subject, as well as the ways in which techniques developed in one area can be applied in other domains for which they were not intended to be used, to begin with.

4.1 What are Anomalies?

A pattern in the data that does not conform to a well-defined concept of typical behavior might be referred to as an anomaly. Figure 2 depicts anomalies in a basic two-dimensional data collection. Since the majority of the observations fall inside these two normal regions, the data have two normal regions labeled N_1 and N_2. Anomalies can be identified at points that are located in regions that are separated from the regions by a sufficient distance, such as points o_1 and o_2, as well as points in region O_3.

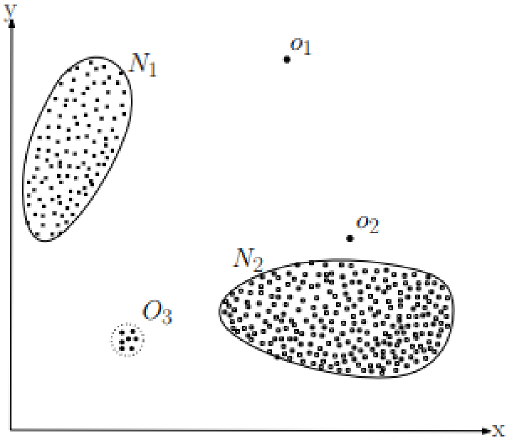

Figure 2: Anomalies in a 2-dimensional data set

Anomalies can be introduced into the data for several different reasons, such as fraudulent activity (like credit card fraud), cyber-intrusion, terrorist activity, or the breakdown of a system;

however, the one thing that all of these reasons have in common is that they are interesting to the analyst. A fundamental aspect of anomaly identification is determining whether or not an abnormality has "interestingness" or real-world significance. The processes of noise removal and noise accommodation, which both focus on getting rid of undesired noise in the data, are linked to anomaly detection, but they are not the same. A phenomenon in the data that is not of interest to the analyst and that acts as a barrier to the analyst's ability to do data analysis are referred to as noise. The necessity to clear the data of undesired elements drives the process of removing noise. This must be done before any data analysis can be carried out. In the context of statistical modeling, "noise accommodation" refers to the process of "immunizing" estimates against "anomalous observations." A second topic that is linked to anomaly detection is novelty detection, which seeks to identify previously undiscovered (emergent, novel) patterns in the data. One example of this would be a new topic of debate in a newsgroup. Anomaly detection and novelty detection are both connected topics. A novel pattern is differentiated from an anomaly by the fact that once identified, novel patterns are normally included in the conventional model. Anomalies, on the other hand, are not. It is important to note that solutions for the linked problems stated above are frequently utilized for anomaly detection and vice versa. As a result, these solutions are examined further in this study as well.

5. SDN-BASED ANOMALY DETECTION FRAMEWORK

In this section, some basic information regarding SDN is presented, and then the operation of the proposed SDN-based anomaly detection framework for suspicious flow identification in social multimedia is discussed.

- **Data Plane:** The data plane is made up of FEs that carry out their operations in accordance with the instruction set (which the controller supplies and which contains instructions for packet forwarding). It is possible to obtain data from network traffic at a desired degree of granularity using FEs that have OF enabled. Within this context, the traffic is conceptualized as flows (a group of packets that share some common features such as addresses, transport protocol, and both source and destination ports). The instruction set that is set up on the FEs is mapped with the list of flow tables, and these flow tables are connected via a pipeline. Accessing the flow tables, configuration, and statistics of the data plane is therefore necessary for the transmission of packets. This process is governed by the OF protocol. FEs on the data plane act as data forwarding devices and routinely transmit messages to controllers to advise them of the current state of ongoing flows. Whenever a packet arrives at a FE, the flow entry that corresponds to that packet is updated. Since it is the responsibility of this module to gather data on traffic, it may be regarded as a requirement for the process of anomaly detection.

- **Control Plane:** This is the decision-making plane of the SDN, and it governs the entire operations of the controller. Some of these functions include system configuration, management, and the interchange of information about routing tables. This plane is the location of all of the control instructions and logic that are utilized in the process of programming the functionalities of FEs. In this configuration, the controller is responsible for managing the whole flow of traffic across an open interface and providing unified choices on flow forwarding, routing, and the discarding of packets. The primary function of the control plane is to determine how the flow tables in the data plane should be set up. At this location, the routing and switching procedures that are needed to synchronize the dispersed flow tables are carried out.

- **Application Plane:** It is mostly made up of programs geared for end users, such as video streaming, online surfing, security implementation, network virtualization, mobility management, load balancing, and so on. In addition to that, it incorporates SDN-based applications including the execution of policies, administration of networks, and security services. The SDN controller is in charge of directing these application flows.

6. CONCLUSION

A quick increase in income is critical for the present cellular network. One option to meet these needs is OTT services. Over-the-top (OTT) service providers, however, depend on QoS to attract customers. The QoS can only be met if service providers' networks are versatile enough to accommodate the needs of their customers. Flexible, elastic, and data-friendly solutions have been the subject of many studies. However, there are still technological hurdles to overcome because of convoluted communication settings. In this thesis, we investigate how SDN may be used to effectively manage resources in order to guarantee quality of service for over-the-top (OTT) apps that produce massive amounts of traffic. A service-oriented cellular network for elephant over-the-top (OTT) applications was the subject of this research and introduction to new ideas. Improved throughput and latency for applications have been suggested concerning several aspects of a future cellular network, such as software-defined networking (SDN), multipath, and heterogeneous communication.

REFERENCES

1. A. Alnoman and A. Anpalagan (2019), "An SDN-Assisted Energy Saving Scheme for Cooperative Edge Computing Networks," 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9013409.

2. A. Malik, R. de Fréin, M. Al-Zeyadi and J. Andreu-Perez (2020), "Intelligent SDN Traffic Classification Using Deep Learning: Deep-SDN," 2020 2nd International Conference on Computer Communication and the Internet (ICCCI), pp. 184-189, doi: 10.1109/ICCCI49374.2020.9145971

3. Tuan, N.N., Hung, P.H., Nghia, N.D., Tho, N.V., Phan, T.V. and Thanh, N.H., (2020)," A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," Electronics, 9(3), 1-7

4. Tuan, N.N., Hung, P.H., Nghia, N.D., Tho, N.V., Phan, T.V. and Thanh, N.H.,(2020)," A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN,"Electronics,9(3),1-14

5. Hai Tao et al. (2022)," SDN-assisted technique for traffic control and information execution in vehicular ad-hoc networks," Computers and

Electrical Engineering, Volume 102, 108108

6. S. A. Kulkarni, V. P. Gurupur and C. King (2022), "Impact Analysis of Stacked Machine Learning Algorithms Based Feature Selections for Deep Learning Algorithm Applied to Regression Analysis," SoutheastCon 2022, pp. 269-275, doi: 10.1109/SoutheastCon48659.2022.9764105

7. S. boukria and M. guerroumi (2019), "Intrusion detection system for SDN network using deep learning approach," 2019 International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS), pp. 1-6, doi: 10.1109/ICTAACS48474.2019.8988138

8. Ombase, P.M., Kulkarni, N.P., Bagade, S.T. and Mhaisgawali, A.V., (2017),” DoSattack mitigation using rule-based and anomaly-based techniques in software-defined networking," In International Conference on Inventive Computing andInformatics (ICICI),469-475

9. Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M. and Karimipour, H.,(2017),” Cyber intrusion detection by combined feature selection algorithm,” Journal ofinformation securityandapplications,44,80-88

10. Mousavi, S.M. and St-Hilaire, M., (2018),” Early detection of DDoS attacks against software-defined network controllers,” Journal of Network and Systems Management, 26(3),573-591

Author’s Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification / Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright / Patent/ Submission for any higher degree or Job/ Primary Data/ Secondary Data Issues, I will be solely/entirely responsible for any legal issues.I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Rounak R. Gupta
Dr. Pramod Sharma

*****