International Journal of Research in Engineering, Science and Management
Volume-2, Issue-6, June-2019
www.ijresm.com | ISSN (Online): 2581-5792

Security and Privacy of Big Data

S. Keerthi[1], J. Sumitha[2]
[1]Department of Software System, Sri Krishna Arts and Science College, Neyveli, India
[2]Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, India

***Abstract*: In big data networks the quality of services is provided which is important along with the security and privacies which are provided by the big data analytics. To reveal the patterns trends and associations, especially relating to human behaviors and interactions big data is extremely large data sets that may be analyzed technically. It is the way to analyze to extract the information from or otherwise deals with data set that is too large or complex to be dealt with data processing application software. Its mechanism is to compare threads and their defense that help to migrate the network vulnerabilities from big data and software defined networks (SDN).**

***Keywords*: bigdata**

1. Introduction

Big data is emerging with social media networks from applications that are been collected in every day's data. Studies have shown that by 2020 the world will have increased 50 times the amount of data with had in 2018 which was currently 1.8 zetta bytes. This sharp increase is due to the data stored over the years that simply come down to cost of storage. The IT industry has decided to make the cost of storage cheap that applications are capable of saving data at exponential rates. Many big data application work in real time. Hence these applications have to create, store and process large amount of information which produces a great deal of volume and demand on the network. It includes network topology, algorithms, security, data retrieval and privacy issues. In IT sectors the resources are capable of handling email, web browsing, and video streaming to become strained. Providing security and privacy has also become a major concern in big data as many critical and real time applications are developed which are based on big data paradigm. This paper fully about the big data network security. It focus on three network security technologies and classifying threads related to security and privacy issues and what type of defense mechanism can be implemented to help the network vulnerabilities from big data and SDN.

A. Security and privacy

It is of three types they are:

- Intrusion detection
- Thread monitoring system
- Flow based NIDS

In this paper we are going to see about the security and privacy issues of intrusion detection briefly.

2. Intrusion detection

Most of the systems use user IDs and passwords as the login patterns to authenticate users. Many users share their login patterns with co-workers and request these co-workers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors are launched from the outer world of the system only. The features of an attack are analyzing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns. Therefore, a security system, named the An Internal Intrusion Detection System (IIDS), is proposed to detect insider attacks at SC level by using data mining and pattern matching techniques. The IIDS creates user's personal profiles to keep track of user's usage habits as their security features and determines whether a valid login user is the account holder or not by comparing user's current computer usage behaviors, it can prevent a protected system from insider attacks effectively and efficiently.

3. Existing of intrusion detection

Computer systems have been widely employed to provide users with easier and more convenient lives. When people exploit powerful capabilities and processing power of computer systems, security has been one of the serious problems in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously, e.g., stealing critical data of a company, making the systems out of work or even destroying the systems. Generally, among all well-known attacks such as harming attack, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack, insider attack is one of the most difficult ones to be detected because firewalls and intrusion detection systems (IDSs) usually defend against outside attacks. Most systems check user ID and password as a login pattern to authenticate users, currently. However, attackers may install Trojans to pilfer victim's login patterns or issue a large scale of trials with the assistance of a dictionary to acquire user's passwords. When successful, they may then log in to the system, access user's private files, or modify or destroy system settings. In a real-time manner a known intrusion can discover the most current host-based security systems and network-based IDSs. It is very difficult to identify who the attacker is because attack packets are often issued with forged IPs or attackers may enter a system with valid login patterns. In detecting attackers and identifying users OS-level system calls (SCs) are much more helpful.

4. Proposed system of intrusion detection

The proposed system offer a security system, named An Internal Intrusion Detection System (IIDS), that detects malicious behaviors launched toward a system at SC level. The IIDS uses data processing and rhetorical identification techniques to mine supervisor call instruction patterns (SC patterns) outlined because the longest supervisor call instruction sequence that has repeatedly seem many times during a user's log file for the user. The user's rhetorical options outlined as associate degree SC pattern oftentimes showing during a user's submitted SC sequence however seldom getting used by different users. The system got to study the SCs generated and also the SC-patterns made by these commands in order that the IIDS will find those malicious behaviors issued by them so stop the protected system from being attacked.

5. Solution

In order to mitigate big data intrusion detection challenges it is important to try different approaches to help to solve the problem. It may be possible to explore being able to implement new features into intrusion detection that can help use signature matching more flexibly, such as utilizing dynamic parameters in IDS signature. It must be processed efficiently at a fast response and real time classification. It can also be helpful to introduce additional intrusion detection mechanism for example: context-aware list-based packet filter and frequency based exclusive signature matching

Eg: ip match on the black or white list.

6. Conclusion

Along with network requirements such as network resiliency, congestion, performance consistency, scalability and partitioning, providing security and privacy must be considered while implementing and infrastructure for big data analytics. As current data infrastructure lacks the characteristics to implement big data network it is important to implement various tools, methods and techniques into network in order to help support big data processing. These tools and approaches helps to manage and process the data more effectively by breaking up the work to distribute simultaneously across the network. In conclusion this paper presents an overview of security and privacy issues of intrusion detection in big data, especially to explore network security concern and mitigation strategies.

References

[1] Anna Sperotto. "Flow-Based Intrusion Detection," Ph.D. Thesis, Centre for Telematics and Information Technology, University of Twente, 2010.
[2] Kvernvik Tor and Matti Mona. "Applying big-data technologies to network architecture", Ericsson Review, 2012.
[3] Guohui Wang, T. S. Eugene Ng, and Anees Shaikh, "Big data tutorial: Everything you need to know".
[4] www.wikipedia.com
[5] www.3Schools.com
[6] www.studymafia.com
[7] www.techwalla.com
[8] www.ukessays.com
[9] www.brighthub.com