International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

Anomaly and Signature Based Intrusion Detection System using Data Mining

Prasann Bharati [1], Dr.Shyam Gupta [2]

P.G. Student, Department of Computer Engineering, Siddhant College of Engineering (SCOE), Pune, India[1]

Associate Professor, Department of Computer Engineering, Siddhant College of Engineering (SCOE), Pune, India[2]

ABSTRACT: The insider attackers i.e. viruses, malwares are a genuine risk to the Internet. With the help of APT malware, attackers can remotely control infected machine and steal the personal information. The malwares, who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviours launched from the outside world of the system only. Some studies claimed that analysing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns are the features of an attack. Introducing a security system, named the Internal Intrusion Detection and Protection System (IIDPS). The proposed novel system placed at the network departure guide that points toward effectively and efficiently detects malware infections based on traffic analysis. To detect suspicious malware we set some rules or dataset which contains suspicious malicious anomaly features by analysis method, and afterward analyse the traffic of the comparing suspicious IP utilizing anomaly-based and signature based detection innovation.

KEYWORDS: Intrusion Detection, Malware Infections, Insider Attack.

I.INTRODUCTION

The computer systems have been widely employed to provide users with easier and more convenient lives. However, 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 pharming 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. To authenticate users, currently, most systems check user ID and password as alogin pattern. However, attackers may install Trojans to pilfer victims login patterns or issue a large scale of trials with the assistance of a dictionary to acquire users passwords. When successful, they may then log in to the system, access user'sprivate files, or modify or destroy system settings. However, 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.

Network related security is becoming a progressively more important issue, since the rapid development of the Internet. Network Attack Detection System (IDS), as the key security defending approach, is widely used against such malicious attacks. Infomining and machine learning technology has been widely applied in network attack detection and prevention systems by discovering behavior habits from the network traffic data. Association rules and sequence rules are the key technique of data exploration for intrusion detection.

The virus attacks are increasing on the online nowadays. Unfortunately, they are difficult to discover a malware andthe infections. This can be a continuous or persistent hacking processes and set of stealthy highlighting on a particular organization with high-value information, for example, government, military and the monetary business. The aim of a virus/malware is to steal the information rather than to make harm the association or system. Once installing to be able to hack in to the system has been accomplished, malware on the contaminated machine by attacker. For example, malware is, Trojan horse or backdoor secondary passage, is custom-made for firewalls and antivirus software of the focus on network. It is not simply utilized for remotely handling the traded off machine in the APT harm, additionally of stealing sensitive information from extended period of time.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

II.RELATED WORK

1. Bogus Biter: A transparent protection nagainst phishing attacks
   Authors: C. Yue and H. Wang

They propose a new approach to protect against phishing attacks with bogus bites. We develop BogusBiter, a unique client-side anti-phishing tool, which transparently feeds a relatively large number of bogus credentials into a suspected phishing site. BogusBiter conceals a victim's real credential among bogus credentials, and moreover, it enables a legitimate Web site to identify stolen credentials in a timely manner. Leveraging the power of client-side automaticphishing detection techniques, BogusBiter is complementary to existing preventive anti-phishing approaches.

Advantages: Transparently protect against phishing attacks.

Limitation: Firefox 2 Web browser.

2. A model-based approach to self-protection in computing system
   Authors: Q. Chen, S. Abdelwahed, and A. Erradi

This project an autonomic model-based cyber security management approach for the Internet of Things (IoT) ecosystems. The approach aims at realize a self-protecting system, which has the ability to together estimate, detect, and respond to cyber-attacks at an early stage. Proposed model-based techniques including: 1) data analysis to recognize and categorize attacks; 2) real-time evaluation and baseline security controls to predict and eliminate potential cyber-attacks; and 3) a multi criteria optimization method to select the most advantageous active response for deploying countermeasures while maintaining system functions. Advantages: Protecting a Web-based application against known and unknown attacks with little or no human interference.

Limitation: Required signatures of unknown attacks in real time.

3. Intrusion detection and identification system using data mining and forensic techniques
   Authors: F. Y. Leu, K.W. Hu, and F. C. Jiang

As using intrusion detection systems and firewalls identify and isolate harmful behaviors generated from the outside world we can find out internal attacker of the system only. In some of the studied define examine that system calls generated by some commands and these command help to find detect accurate attacks, and attack patterns are the features of an attack. However in the paper security System defines as the Internal Intrusion Detection and Protection System (IIDPS), is help to detect internally attacks by using data mining and forensic technique at SC level.

Advantages: To detect internally attacks by using data mining and forensic technique at SC level.

Limitation: To detect and prevent insider attacks.

4. Detecting web based DDoS attack using MapReduce operations in cloud computing environment
   Authors: J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim

This study proposes a method of integration between HTTP GET flooding among DDOS attacks and Map-Reduce processing for a fast attack detection in cloud computing environment. This method is possible to ensure the availabilityof the target system for accurate and reliable detection based on HTTP GET flooding.

Advantages: The processing time for performance evaluation compares a pattern detection of attack features with the Snort detection.

Limitations: Proposed method is shorter with increasing congestion.

5. The use of computational intelligence in intrusion detection systems
   Authors: S. X. Wu and W. Banzhaf

Intrusion detection based upon computational intelligence is currently attracting considerable interest from the research community. Characteristics of computational intelligence (CI) systems, such as adaptation, fault tolerance, high computational speed and error resilience in the face of noisy information, fit the requirements of building a good intrusion detection model. Here we want to provide an overview of the research progress in applying CI methods to the problem of intrusion detection. The scope of this review will encompass core methods of CI,

including artificial neural networks, fuzzy systems, evolutionary computation, artificial immune systems, swarm intelligence, and soft computing.

Advantages: The findings of this review should provide useful insights into the current IDS literature and be a good source for anyone who is interested in the application of CI approaches to IDSs or related fields.

Limitation: Computational intelligence methods to the problem of intrusion detection.

III.METHODOLOGY

The proposed system based on the traditional IDS based on rule detection, intrusion mode is usually pre-defined by the security experts. The advantage of this approach is that the rules can be formulated to detect specific attacks. Therefore, it is guarantee to detect known attacks and produce few alarms for attack. However, facing with increasing and changing net- work data flow, it is impractical to discover various intrusion modes punctually. The anomaly detection is presented due to this reason. New attacks can be detected in time which the system has unobserved before as they deviated from normal behaviour. However, current anomaly detection schemes still suffer from a high rate of false alarms. Additionally, system introduces the recovery of the lost data by keeping the copy of infected file at the time of attack attempt by malware which also achieves the data integrity and freshness in the network traffic. At first senders the sender will send the multiple files the, here the sender knowingly add some malicious content to file which may affect the other files as well the receiver side files. Once that files are received at IDS, the IDS may be

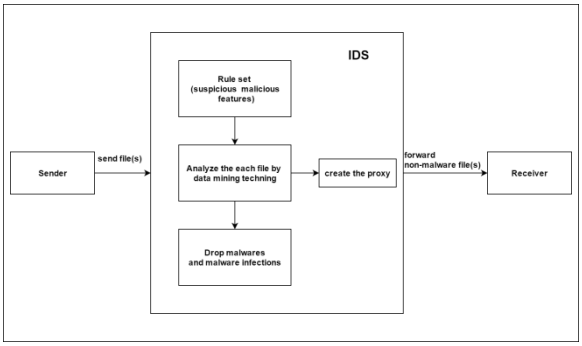

Fig. 1. System Architecture

present at the receiver node or may be at network egress so that to provide the security by analysing the network traffic. In the network traffic the malicious file will affect the other normal file also. Once the infection is performed at that only the proxy of that victim file is created and saved at IDS system. The IDS will detect the malicious file based on the rules list available which contains the features of malicious files like suspicious anomalies such as malware, virus, worms etc. after detection and the IDS will send the files to receiver by dropping the malicious files and infected files and provide the recovery of infected file in the form of proxy available at the time of attack.

Mathematical Model

Let W be the whole system which consist: W = Input, Process, and Output.
Where,

- Input is the input given to the system.
- Process is the procedure or working of the system after giving the set of input.
- Output is the expected outcome of the system.

Input = {S, IDS, R, F, FR, IF, L, AES}
Where,

- S is the sender.
- An ID is intrusion detection system.
- R is the receiver.
- F is the set of files.
- FR is the file recovered or proxy.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

- IF be the infected file.
- L is the malicious features rule set.

Process:

Step 1: initially IDS will load the rule set of malicious features such as malware, virus, worms etc. which is used to classify and detect the malicious files in the network traffic which may affect to receiver.

This IDS is placed at network egress point or at particular node who act as receiver.

Step 2: Sender S will send the set of files.

i.e. F = f1, f2,… fn.

Each file will be encrypted and send to receiver by using AES-256 bit algorithm to achieve for providing security to the data.

Once the sender sends the files F, if that file contains the malicious content or features then that file will affect the another normal file. At this time only the system will creates the replica of that file.

Step 3: Once the files F received at IDS, the DS will apply the AES-256 algorithm for decryption because it is difficult to identify the malicious features in the encrypted form then system will apply the classification on files to detect malicious content file based on rules set. It will drop the malicious feature/ content files as well as malicious infections.

Step 4: the IDS will again decrypt the normal files and send to receiver.

Step 5: the receiver will receive the normal files in the form of normal plain text form.

IV. EXPERIMENTAL RESULTS

Output:

Detection of malicious infections and recovery of file by means of keeping the

A. Advantageous of Proposed System:

1. A novel system placed at the network edge intrusion detection technology to detect malware infections inside the network.
2. Accurate detection of malwares by using rule set for classification.
3. Achieves the data integrity.

B. Applications:

1. This system can implemented in network edge for detection malwares in wireless communication where data integrity is needed.
2. In confidential message passing.

C. Algorithm: AES-256

AES (Advanced Encryption Standard) is a symmetric encryption algorithm. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. Implementing AES encryption algorithm for encrypting the data at sender node as well as IDS and decryption is done at IDS as well as receiver node for the security purpose.

D. Result Analysis:

Input:

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the Time and performance of system based on this attributes we getting following result for our proposed system.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 8, August 2020||

Parameter	Existing	Proposed
Security	7	10
Accuracy	5	10
Recovery	1	10
Sustainability	4	10

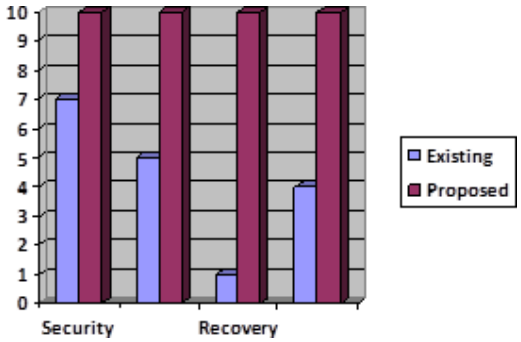

Fig. 2. Expected Result Analysis

V.CONCLUSION

In this, proposed a system which is placed at the network egress points to detect malware infections inside the network combined with network traffic analysis. The system processes advantages of high efficiency and accuracy. Additionally the system can achieves the data integrity by means of recovery of infected file and accurate detection of malware content file. The experimental results show that this security approach is practicable for improving the supportable of the system and is good at detecting virusinfections.

VI.ACKNOWLEDGEMENT

I would prefer to give thanks the researchers likewise publishers for creating their resources available. Additionally, I appreciative to commentator for their vital recommendations moreover Im conjointly grateful to reviewer for their valuable suggestions and also thank the college authorities forproviding the required infrastructure andsupport.

REFERENCES

[1] C. Yue and H. Wang, BogusBiter: A transparent protection against phishing attacks, ACM Trans. Int. Technol., vol. 10, no. 2, pp. 131, May 2010.
[2] Q. Chen, S. Abdelwahed, and A. Erradi, A model-based approach to self-protection in computing system, in Proc. ACM Cloud Autonomic Comput.Conf.,Miami,FL,USA,2013,pp.110.
[3] F. Y. Leu, K.W. Hu, and F. C. Jiang Intrusion detection and identification system using data mining and forensic techniques, Adv. Inf. Comput. Security,vol.4752,pp.137152,2007.
[4] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environment, J. InternetServ.Inf.Security,vol.3,no.3/4,pp.2837,Nov.2013.
[5] S. X. Wu and W. Banzhaf, The use of computational intelligence in intrusion detection systems: A review, Appl. Soft Comput., vol. 10, no. 1, pp. 135, Jan.2010.
[6] P. Angin and B. Bhargava, An agent-based optimization framework for mobile-cloud computing, J. Wireless Mobile Netw., Ubiquitous Comput., DependableAppl.,vol.4,no.2,pp.117,Jun.2013.
[7] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, Biometric authen- tication using mouse gesture dynamics, IEEE Syst. J., vol. 7, no. 2, pp. 262274, Jun.2013.