INTRUSION DETECTION SYSTEM FOR CLOUD BASED ON NAIVE BAYES AND HASHING

Amruta Deshmukh[1], Kirti Girdhani[2], Nayan Keskar[3], Prajakta Gite[4], Prof. D. D. Sharma[5]

Department of Computer Engineering,
Late G.N.Sapkal College of Engineering, Anjaneri, Nashik.

***Abstract*: Network traffic in the cloud computing environment is characterized by large scale, high dimensionality, and high redundancy, these characteristics pose serious challenges to the development of cloud intrusion detection systems. Deep learning technology has shown considerable potential for intrusion detection. Therefore, this study aims to use deep learning to extract essential feature representations automatically and realize high detection performance efficiently. An effective stacked contractive autoencoder (SCAE) method is presented for unsupervised feature extraction. By using the SCAE method, better and robust low-dimensional features can be automatically learned from raw network traffic. We are creating a system that allows user to provide security to their files and protect them from hacker and avoid the malicious attacks, we are encrypting the password by hash and also if the hacker break are hash code it will get only the dummy data, otp will also will there for authentication.**

***Keywords*: Information Security, Intrusion Detection, Data Mining**

INTRODUCTION

Designers depend on the instruments given by their IDE to peruse and explore an enormous programming framework. These components are typically founded simply on a framework's static source code. The static point of view, nonetheless, isn't to the point of understanding an item arranged program's conduct, specifically whenever executed in a powerful language. We propose to improve IDEs with a program's runtime data (e.g., message sends and type data) to help program understanding through exact route and instructive perusing. To definitively indicate the sort and measure of runtime information to accumulate about a framework being worked on, powerfully and on request, we take on a strategy known as halfway conduct reflection. We carried out route and perusing upgrades to an IDE that exploit this runtime data in a model called Hermion. We present starter approval of our trial upgraded IDE by requesting that engineers survey its convenience to comprehend a new programming framework.

MOTIVATION OF THE PROJECT

The current situation of Hindustan Tungsten Carbide organization is very upset the fundamental issue they are confronting right presently is to oversee records. Not able to find the phase of particular material of client. Due to which the commitment to client goes fail.

LITERATURE SURVEY

The rule-based Intrusion Detection and Prevention Model for Biometric System. Modern biometric systems claim to provide alternative solution to traditional authentication processes. Even though there are various advantages of biometric process, it is vulnerable to attacks which can decline it's security. The intrusion detection is an essential supplement of traditional security system. This security system needs the robust automated auditing, intelligent reporting mechanism and robust prevention techniques. We suggest rule based intelligent intrusion detection and prevention model for biometric system. This model contains a scheduler to prepare a schedule to check different logs for possible intrusions, detectors to detect normal or abnormal activity. If activity is normal then alarming and reporting has been executed. If abnormal activity is found the rule engine fires the rule to detect intrusion point and type of intrusion. The model also contains an expert system to detect source of intrusion and suggest best possible prevention technique and suitable controls for different intrusions. This model is also used for security audit as well as alarming and reporting mechanisms. The malicious activity database is stored for future intrusion detection. To detect source tracking backward chaining approach is used. The rules are defined and stored in the Rule engine of the system.[1]

Autonomous rule creation for intrusion detection many computational intelligence techniques for anomaly based network intrusion detection can be found in literature. Translating a newly discovered intrusion recognition criteria into a distributable rule can be a human intensive effort. This paper explores a multi-modal genetic algorithm solution for autonomous rule creation. This algorithm focuses on the process of creating rules once an intrusion has been identified, rather than the evolution of rules to provide a solution for intrusion detection. The algorithm was demonstrated on anomalous ICMP network packets (input) and Snort rules (output of the algorithm). Output rules were sorted according to a fitness value and any duplicates were removed. The experimental results on ten test cases demonstrated a 100 percent rule alert rate. Out of 33,804 test packets 3 produced false positives. Each test case produced a minimum of three rule variations that could be used as candidates for a production system. [2]

Expert systems in intrusion detection: A case study securing the system is a major concern in the present digital era. The wide spread of networking has increased the necessity of protecting the system to a very high extent. Intrusion detection system is

considered as the backbone for securing system/network by intrusions. Intrusion detection system enables us to secure the system from the unauthorized users, who intend to misuse the system. Intrusion Detection system is defined as a solution of system security to identify the abnormal activities in a computer system or network. Different types of techniques, approaches have been deployed within the field of intrusion detection system (IDS). In this paper, a survey on intrusion detection system is carried out. The paper provides an introduction to the concepts of intrusion detection system, a brief survey about the literature, techniques and counter attack methodologies that are used within the intrusion detection system. This survey will provide helpful insight into the related literature of intrusion detection systems. [3]

PROBLEM STATEMENT

Security issues have resulted in severe damage to the cloud computing environment, adversely affecting the healthy and sustainable development of cloud computing. Intrusion detection is one of the technologies for protecting the cloud computing environment from malicious attacks.

PROJECT SCOPE

Security issues have brought about serious harm to the distributed computing climate, antagonistically influencing the sound and economical improvement of distributed computing. Interruption recognition is one of the advancements for shielding the distributed computing climate from malignant assaults.

GOALS AND OBJECTIVE

- To make a system, this is user friendly.
- Security providing to important data of user.
- Avoiding the malicious attacks by hacker.

PROPOSED SYSTEM

Cloud computing is an emerging Internet-based computing model that provides tenants with seemingly “unlimited” IT services, thereby freeing them from complex underlying hardware, software, and protocol stacks. Although “open for all service” is the essence of cloud computing, it does not necessarily comprise useless information. Tenants can use cloud services for efficient computing. However, they can also abuse the cloud environment and attack the network. For example, a malicious tenant may reside in a virtual machine, successfully intrude into other VMs in the cloud, and use the puppet machines to spread malicious software, or launch distributed denial of service attack, and so on. In fact, tenant behavior will generate massive network traffic in the cloud environment, mainly including “north-south” and “east-west” traffic. The “north-south” traffic mainly refers to the traffic of tenants accessing cloud services from the external network, and the “east-west” traffic refers to the traffic between VMs in the virtual network Cisco’s cloud industry research report predicts that the global cloud network traffic will account for 95 percent of the total network traffic by 2021. In particular, the “east-west” traffic between VMs in the cloud environment will account for 85 percent.

SYSTEM ARCHITECTURE

A description of the program architecture is presented. Subsystem design or Block diagram, Package Diagram, Deployment diagram with description is to be presented.

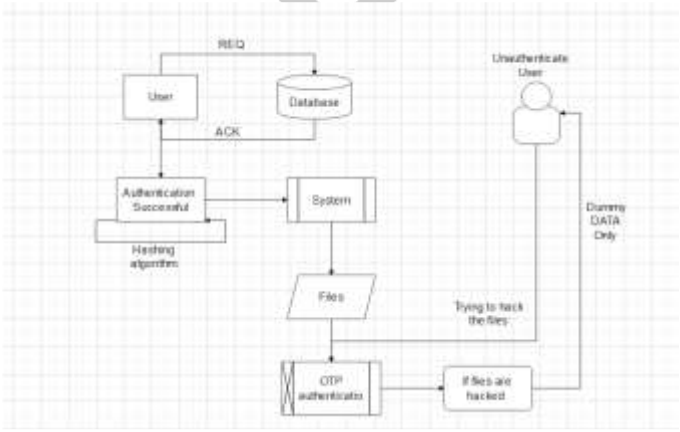

Fig -1: System Architecture Diagram

Network traffic will continue to increase dramatically and will inevitably encounter malicious attacks. Network attacks not only result in severe damage to the cloud environment but also cause tenants to lose confidence in cloud computing itself, which will adversely affect the healthy and sustainable development of cloud computing. Intrusion detection is one of the technologies for protecting cloud computing from malicious attacks.

ADVANTAGES

1. User friendly system
2. Hacking secure
3. Centralized system
4. Security providing to important data of user
5. Avoiding the malicious attacks by hacker

APPLICATION

1. Industrial
2. Banking
3. Government Security Agencies

CONCLUSION

An Intrusion detection system is a component of the defensive operations that complements the defenses such as firewalls. The Intrusion detection system mainly detects attack signs and then alerts the system for such instructions and send the dummy data only to attackers/ hackers. According to the detection method, Intrusion detection systems are usually categorized as misuse detection and anomaly detection systems. The operation point of view, they are be classified in network based or host based IDS. In current Intrusion detection systems information is composed from both network and host resources. In terms of presentation, an Intrusion detection system becomes more correct as it detects more attacks and and send to the dummy data to hackers. Hence We are making a framework that permits client to give security to their documents and shield them from programmer and stay away from the noxious assaults , we are encoding the secret word by hash and furthermore if the programmer break are hash code it will get just the fake information, OTP will likewise will there for confirmation ,we are overcoming the drawback of existing system , and providing a smart system that will not only monitor and control our data with security but also supply it to whenever necessary.

REFERENCES

[1] Maithili Arjunwadakr and R.V. Kulkarni, ”The rule-based Intrusion Detection and Prevention Model for Biometric System”, Journal of Emerging Trends in Computing And Information Sciences, OCT 2010.

[2] Todd Vollmer, Jim Alves-Foss and Milos Manic, ”Autonomous rule creation for intrusion detection”, 2011 IEEE Symposium on Computational Intelligence in Cyber Security.

[3] M. Sebring, E. Shellhouse, M. Hanna and R. Whitehurst, ”Expert systems in intrusion detection: A case study”, Proceedings of the 11 th National Computer Security Conference, pp. 74-81, 1988

[4] T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Edwards P. Neumann, et al., IDES: The Enhanced Prototype. A Real-Time Intrusion Detection System, 1988.

[5] D. Anderson, T. Lunt, H. Javitz, A. Tamaru and A. Valdes, Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES).