INTRUSION DETECTION SYSTEM

Begimov O‘ktam Ibragimovich
PhD, associate professor, Alfraganus University, Tashkent, Uzbekistan
uktam1985beg@mail.ru
Bo‘riboyev Tolibjon Mirali o‘g‘li
Alfraganus University, Tashkent, Uzbekistan
buriboevtolib@gmail.com

MAQOLA MALUMOTI

MAQOLA TARIXI:
Received: 05.11.2025
Revised: 06.11.2025
Accepted: 07.11.2025

KALIT SO’ZLAR:
IDS,NIDS,HIDS,KDD cup 1999 data set, neural network.

ANNOTATSIYA:

Intrusion detection system has become a very necessity in computer network era. Now a days it is expanding day by day.security has become a vital issue for modern computer systems.Exchange of data in any communication process is very essential and its security is very important in any network because of the increase in unauthorized accesses and attacks. Intrusion Detection system plays a major role in computer security that can be classified as Host-based Intrusion Detection System (HIDS), which protects a certain host or system or an application, Network-based Intrusion detection system (NIDS), which protects a network of hosts and systems,Anomaly based Intrusion detection system and Signature based misuse. There are several Intrusion detection system techniques for both anomaly and misuse intrusion detection. In this paper we described many research on various types of attacks and different kinds of intrusion detection system.

Introduction

The Internet is exceptionally efficient and cheap method of communication in every important field of life. With the expanded utilization of system engineering, its security has gotten to be extremely basic issue as the machines in distinctive connection holds very secure data and sensitive information. Be that as it may, the Internet Protocol (IP) on which the entire web is based is extremely insecure and vulnerable to viruses and hackers. Many methods have been developed to secure the network infrastructure and communication over Internet. Some of them are the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. A Network Intrusion is a suspicious and sudden deviation from the ordinary behaviour of the system. The Intrusion undermines the confidentiality, integrity and security of a network system.

IDS is a gadget that is set inside a secured system to screen what happens inside the system.The intrusion detection system is useful not only in detecting successful intrusions, but also in monitoring or preventing the attacks for timely countermeasures. IDS are classified mainly in four types: Anomaly based Intrusion Detection System, Signature based Misuse, Host based Intrusion Detection System(HIDS), Network based Intrusion Detection System(NIDS).

Anomaly based Intrusion Detection System: Anomaly Intrusion Detection is based on the normal behaviour of a subject (e.g. a system or a user). Any action that considerably deviates from the normal behaviour is considered as intrusive. The main advantage of anomaly detection system is that they can detect previously unknown attacks.

Signature based Misuse:ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack.Most signature analysis systems are based on simple pattern matching algorithms.

Host based Intrusion Detection System:A host-based IDS runs under a customer or host workstation to secure that particular host, host operating system or the application logs in the audit information. It is a system which analyses the internals of a computing system as well as the network packets on its network interfaces. This was the first type of intrusion detection software to have been designed, to secure the system where outside interaction was infrequent.

Network based Intrusion Detection system:A network based IDS is a stand-alone mechanism appended to the system to screen movement all around that system .This IDS looks for attack signatures in network traffic via a promiscuous interface.A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

The second section presents description of KDD 99 dataset with types of attacks. The third section describes the literature survey. Finally, the paper is concluded in the fourth section.

Kdd cup 1999 data set

There is specifically extracted information situated is KDD data set with the end goal of experiments with intrusion detection problems. KDD information set hold 42 connection records. As a rule intrusion detection framework utilizes all the connection records accessible in the information with the end goal of the intrusion detection.KDD cup 1999 dataset was concentrated from 1998 DARPA Intrusion detection evaluation program managed by MIT Lincoln labs.The KDD training dataset consist of 10% of original dataset that is approximately 494,020 single connection vectors each of which contains 41 features and is labeled with exact one specific attack type i.e., either normal or an attack. Each vector is labeled as either normal or an attack, with exactly one specific attack type. Deviations from „normal behavior“, everything that is not „normal“, are considered attacks.

There are several attacks in any network.KDD CUP99 has been most widely used in attacks on network.The most widely used classification for attacks in the research communities is the one adopted by K. Kendall. This classification categorizes the computer attacks into:

DOS Attacks: Denial of service (DOS) attacks try to render the system or certain service unstable.(e.g. Syn flood).

User to Root: it tries to gain the root or admin privilege from normal user privilege.(e.g. various “buffer overflow” attacks).

Remote to User: it tries to gain local account privilege for unauthorized entity.(e.g. guessing password).

Probes: In probing, attacker scans a machine or a network device for gathering the information about weaknesses or vulnerabilities that can be exploited later to compromise the target system. Example: saint, mscan, nmapetc.

Category	Class label(attack) in dataset
DOS-Denial of service	back,land, pod, neptune, smurf, teardrop
R2L-Remote to local	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient
U2R-User to root	Buffer_overflow, loadmodule, perl, rootkit
Probe	Ipsweep, nmap, portsweep, satan

Types of attacks that are grouped into four main types tabulated in Table I.

Table 1. Category of Attacks in KDDCUP99 Dataset

The data citing to a bunch of packets over a time length of two seconds, additionally named as packet data, lay down in KDD Cup99 have forty one (41) features. Among these forty one features, 1 to 9 are utilized to illuminate basic features of a packet, 10 to 22 concentrate on content features, 23 to 31 are employed for traffic features with 2 seconds of your moment window and 32 to 41 for host primarily based features. They are essentially classified into three categories: basic features of individual connection, content features contained by a connection, and traffic features that are computed employing a two seconds time window. Although several irregularities are existed in KDD Cup 99 data set, analysis activities in IDS area unit still are using the KDD Cup 99 dataset for analysing and exploring new approaches for higher IDS. Hence, the projected technique has been experimented and analysed with KDD Cup 99.

Literature survey

Now a days Intrusion detection system has become essential part to detect various type of attack in network or a system. A number of methods and techniques have been proposed as

many systems have been affected by a variety of intrusions. Novel Intrusion Detection System integrating layered framework with Neural Network.The Hidden Markov Model is used to implement and determine the system call based anomaly intrusion detection.

Conditional Random Fields and Layered Approach are addressed by the two issues of Accuracy and Efficiency. This approach demonstrates the high attack detection accuracy and high efficiency using Conditional Random Fields and Layered Approach. This approach uses KDD Cup ‟99 intrusion detection data set for detecting the attacks. Neural network approach for intrusion detection Intrusion Detection System, has the fact that an intruder‟s behaviour is different from a legitimate user‟s behaviour. This paper proposes a neural network approach to improve the alert throughput of a network and making it attack prohibitive using IDS. This system is experimented with KDD CUP 99 dataset.

Attacks Classification in Adaptive Intrusion Detection using Decision Tree it is also experimented with KDD99 and proves that proposed system achieved 98% attack detection.Intrusion Detection Systems Using Decision Trees and Support Vector Machines represents the decision tree data mining techniques as an intrusion detection mechanism are investigated and evaluated and compared it with Support Vector Machines (SVM). Intrusion detection with Decision trees and SVM were tested with benchmark 1998 DARPA Intrusion Detection data set. It shows that Decision trees gives better overall performance than the SVM. Analysis and Design for Intrusion Detection System Based on Data Mining Naïve Bayes classifiers provide a very competitive result even this classifier having a simple structure on his experimental study. According to the author, Naïve Bayes are more efficient in classification task.Performance Comparison For Intrusion Detection System Using Neural Network With Kdd Dataset,In the proposed research the four types of classifiers used are Feed Forward Neural Network (FFNN), Generalized Regression Neural Network (GRNN), Probabilistic Neural Network (PNN) and Radial Basis Neural Network (RBNN). The performance of the full featured KDD Cup 1999 dataset is compared with that of the reduced featured KDD Cup 1999 dataset. The MATLAB software is used to train and test the dataset and the efficiency and False Alarm Rate is measured

Feature Selection for Modeling Intrusion Detectioninvestigated the performance of three feature selection algorithms Chi-square, Information Gain based and Correlation based with Naive Bayes (NB) and Decision Table Majority Classifier. Empirical results show that significant feature selection can help to design an IDS that is lightweight, efficient and effective for real world detection systems.Intrusion Detection System,this paper focuses on study of existing intrusion detection task by using data mining techniques and discussing on various issues in existing intrusion detection system (IDS) based on data mining techniques.

Conclusion

This paper concluded with an overview of machine learning technologies which are being utilized for the detection of attacks in IDS and system design of effective IDS. The

security of information in computer based systems is a major concern to researchers. The work of IDS and methodologies which has been a major focus of information security.

References

1. O'.I.Begimov, T.M.Bo'riboyev / Extracting tagging from exocardiographic images via machine learning algorithmics // Analysis of world scientific views International Scientific Journal Vol 2 Issue 1 IF(Impact Factor)8.2 / 2023
2. O'.I.Begimov, T.M.Bo'riboyev / General Theory About the Traditional Methods and Algorithms of Machine Learning // AMERICAN Journal of Public Diplomacy and International Studies Volume 02, Issue 04, 2024 ISSN (E):2993-2157.
3. T.M.Bo'riboyev / Hetnet tizimi asosida avtonobillaring harakat trafigini boshqarish va tahlil qilish // Nejmettin, 03-06 Ekim 2023 tarihlerinde Erbakan Üniversitesi ve Alfraganus üniversitesi öncülüğünde düzenlenen "ipek Yolunun Ötesinde kongreler dizisi: Bir Yol, Bir Kuşak: Göç, turizm ve ekonomi politik Kongresi (SIRCON 2023)" programına sertifika almak için katıldı. (Sayfa 320-324)
4. NIST AI 100-2 E2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations https://csrc.nist.gov/pubs/ai/100/2/e2023/final Проверено: 15.07.2024
5. Perdisci, Roberto, et al. "Misleading worm signature generators using deliberate noise injection." 2006 IEEE Symposium on Security and Privacy (S&P'06). IEEE, 2006.
6. 14 Risks and Dangers of Artificial Intelligence (AI) https://builtin.com/artificial-intelligence/risks-of-artificial- intelligence Проверено 15.08.2024.
7. Song, Junzhe, and Dmitry Namiot. "A survey of the implementations of model inversion attacks." International Conference on Distributed Computer and Communication Networks. Cham: Springer Nature Switzerland, 2022.
8. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final Проверено 15.08.2024.
9. OWASP https://owasp.org/ Проверено 15.08.2024.