Anomaly Based Intrusion Detection System Through Feature Selection Analysis and Building Hybrid Efficient Model

Divya N
PG Student, Department of MCA
PES College of Engineering, Mandya

Prof. K M Sowmyashree
Assistant Professor, Department of MCA
PES College of Engineering, Mandya

Abstract- This project describes the challenge improvement of anomaly-based intrusion detection and prevention system. With the extended dependence of corporations on technological solutions, the cyber threats have turn out to be some of the main issues for the very existence of the businesses. Thus, the safety measures to be carried out want to go past a easy presence of a firewall and anti-malware. In this work, an overview of two Intrusion Detection and Prevention System(IDPS) has been performed. The major intention of this project is to furnish a facts about the intrusion detection, intrusion detection methods, kinds of attacks, awesome tools and techniques, An Intrusion Detection System is used to word all kinds of malicious neighbourhood traffic and laptop utilization that can now not be detected with the aid of capacity of a usual firewall. This consists of neighbourhood assaults in opposition to prone services, data pushed assaults on applications, host exceptionally based totally assaults such as privilege escalation, unauthorized logins and get entry to sensitive files, and malware (viruses, Trojan horses, and worms).

***Keywords*- Machine Learning, Intrusion Detection System(IDS), RSA Algorithm, Email Phishing.**

I. INTRODUCTION

The technological solutions can offer a wide variety of benefits both for individual users as well as for large enterprises, where the primary difference is the actual amount of financial resources that are at the stake if the technology gets exploited by an attacker in an attempt to perform malicious activities against those targets. By integrating web based services into a business model, an organization can increase the accessibility of its business outreach. However, at the same time it makes that organization vulnerable to cyber threats, which can cause them a tremendous financial damage. Thus, the presence of the appropriate configured firewall and regularly up to date anti-malware nonetheless does no longer assurance the safety of the laptop or a community of computer systems and for that reason it's vital to honestly screen the site visitors and discover viable instances of suspicious behaviour. The Intrusion Detection Systems (IDS) would possibly assist to notice and alert about possible assaults with the aid of examining community site visitors and deciding whether or not the found behaviour complies with the predefined allowed conditions. Namely, the IDS can be based totally on the predefined set of signatures of the recognised threats or the modern conduct may want to be in contrast towards a baseline that used to be measured until now in the course of a positive duration of time, in an strive to become aware of feasible anomalies.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

II. LITERATURE SURVEY

While most industries around the world are affected by the looming danger of cyber threats, the banking sector has always been the worst hit. Naturally, this brings upon considerable damages due to the very environment that the banking sector works in-they deal in billions of dollars every single day, trading with a plethora of people and businesses all over the world. They also deal in an incredibly important and vast financial information from multiple customers. Recently, a cyber attack on Cosmos Bank in Pune, India resulted in Rs. 94 crore being stolen. In 2016, Bangladesh Bank, the country's central bank was hacked and the hackers successfully stole 81 Million USD. It was found that hackers used a combination of social engineering technique and viruses to obtain employee credentials to access the bank network and make transfers. Most researches have made an effort to resolve this cyber attack by taking Monitoring System as an example to detect malicious activity with different tools and techniques such as Black watch and Data Mining.

Drawbacks:

- False Positive: Result of an IDS firing an alarm for legitimate network activity.
- False Negative: IDS fails to detect malicious network activity.

Since the current IDS is tuned to detect known service level attack it is essential to build hybrid efficient model which provides a common solution for combination of attacks.

Advantages:

- Fast and efficient system
- Using the proposed system we can protect web clusters from Insider threats and phishing attacks by employing Required techniques.
- More advanced and efficient than existing system.

- It detects abnormality.

III. REVIEW OF RELATED WORK

This section provides an explanation on anomaly based IDS using machine learning technique eg., using Rivest Shamir Adleman(RSA) algorithm in order to detect abnormal behaviour in IDS. The RSA algorithm is the foundation of a cryptosystem --a suite of cryptographic algorithms that are used for particular safety offerings or functions -- which permits public key encryption and is extensively used to impervious sensitive data.

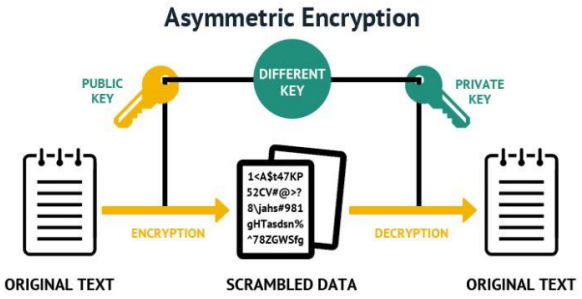


Fig.1 Asymmetric Encryption

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one purpose why RSA has grow to be the most extensively used uneven algorithm: It affords a approach to guarantee the confidentiality, integrity, authenticity, and non-repudiation of digital communications and information storage.

IV. IMPLEMENTATION

This project describes the challenge improvement of anomaly-based intrusion detection and prevention system. With the extended dependence of corporations on technological solutions, the cyber threats have turn out to be some of the main issues for the very existence of the businesses. Thus, the safety measures to be carried out want to go past a easy presence of a firewall and anti-malware. In this work, an overview of two Intrusion Detection and Prevention System(IDPS) has been performed. The major intention of this project is to furnish a facts about the intrusion detection, intrusion detection methods, kinds of attacks, awesome tools and techniques. Taking Banking System as an application enables to detect Insider threats and Phishing attacks on user web. Our main intention to use Hybrid Efficient Model is to provide a common solution for combined attacks.

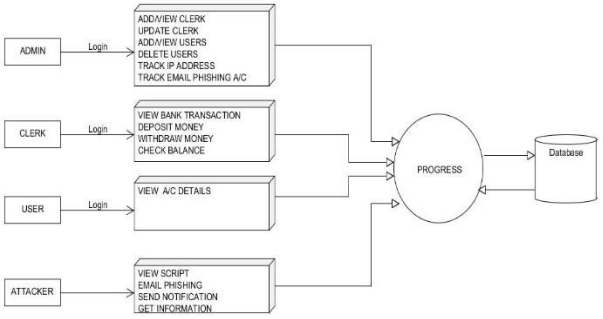
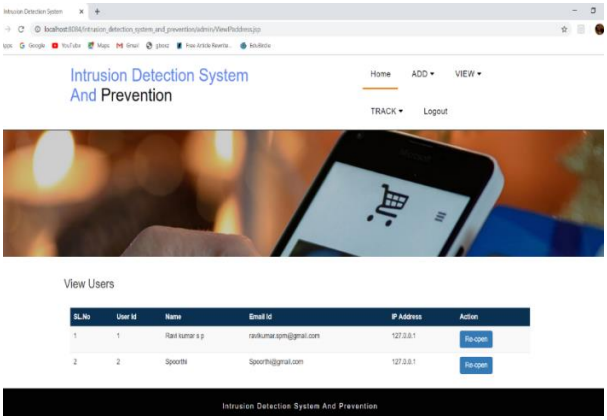
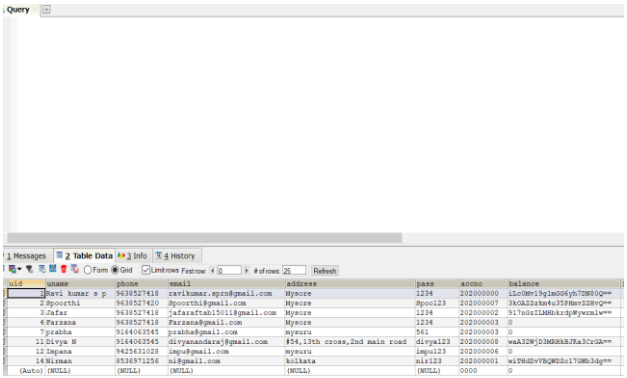


Fig.2 System Implementation

V. RESULT





VI. CONCLUSION

Insider threat assault and phishing assault has grow to be a extreme risk to the protection of net servers. Since these assaults are launched all at once and severely, a quick intrusion prevention machine is appropriate to observe and mitigate these assaults as quickly as possible. In this project, we advise an fantastic intrusion detection system, which leverages the design to rapidly observe and mitigate insider threat assault and phishing attack.

VII. FUTURE ENHANCEMENT

- In future this application can be automated by designing intrusion alert systems, which should be designed carefully.
- The above approach can be further extended to other upstream networks.

VIII. REFERENCES

[1] Lee, W. and Stolfo, S. J., "A Framework for Constructing Features and Models for Intrusion Detection Systems," ACM Transactions on Information and System Security, vol. 3, November, 2000

[2] W. Lee, S. J. Stolfo, and K. W. Mok, “Mining in a data-flow environment: Experience in network intrusion detection”, In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD-99).

[3] W. Lee, S. J. Stolfo, and K. W. Mok, “A data mining framework for building intrusion detection models”, In Proceedings of the 1999 IEEE Symposium on Security and Privacy, May 1999.