An Internal Intrusion Detection and Protection System using Data Mining and Forensic Techniques.

Mali Rohini S.[1], . Unde Shital N[2], Shedge Prajvaleeta T.[3], Prof. Gholap. P.S.[4]

[1] *Student, Computer Engineering, SPCOE, Maharashtra, India*
[2] *Student, Computer Engineering, SPCOE, Maharashtra, India*
[3] *Student, Computer Engineering, SPCOE, Maharashtra, India*
[4]*Assistant professor, Computer Engineering, SPCOE, Maharashtra, India*

ABSTRACT

Around the world, billions of individuals access the web these days. Intrusion detection technology could be a new generation of security technology that monitors system to avoid malicious activities. The IDPS uses a neighborhood procedure grid to sight user's malicious behaviors during a period manner. during this project, the system proposes a security system, named the Intrusion Detection and Protection System at call level, that creates personal profiles for users to stay track of their usage activity because the rhetorical options. The projected work is regarded with forensics technique and intrusion detection mechanism. The bottom paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses varied data processing and rhetorical techniques algorithms for the system to figure in real time. Data processing ways are projected for cyber analytics in support of intrusion detection. During this project, the system designed Internal Intrusion Detection System (IIDS) that implements predefined algorithms or techniques for distinctive the attacks or user's malicious behavior over a network.

Keyword: - *Data Mining, Insider Attacks, Intrusion detection & Protection, System Call, attack patterns, User's Behavior.*

---

1. Introduction

In the past decades, portable computer systems are wide used to provide users with easier and extra convenient lives. However, once of us exploit powerful capabilities and method power of portable computer systems, security has been one in each of the extraordinary problems at intervals the portable computer domain since attackers really generally try to penetrate portable computer systems and behave maliciously, e.g., stealing vital information of a corporation, making the systems out of labor or even destroying the systems. Generally, among all well-known attacks like pharming attack, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack, business executive attack is one in each of the foremost hard ones to be detected as results of firewalls and intrusion detection systems (IDSs) generally defend against outside attacks. To proof users, currently, most systems check user ID and word as a login pattern. However, attackers may install Trojans to snarf victims' login patterns or issue associate degree outsized scale of trials with the assistance of a lexicon to amass users' passwords. Once flourishing, they will then log in to the system, access users' private files, or modify or destroy system settings. As luck would have it, most current host-based security systems associate degreed network-based IDS's will discover an acknowledged intrusion throughout a fundamental quantity manner. However, it's really hard to identify United Nations agency the aggressor is as a results of attack packets unit of measurement typically issued with solid IPs or attackers may enter a system with valid login patterns. the OS-level system calls (SCs) are rather a lot of helpful in detection attackers and distinctive users, method associate degree outsized volume of SCs, mining malicious

behaviors from them, associate degreed distinctive possible attackers for associate degree intrusion unit of measurement still engineering challenges.

1.1 Motivation

- Loses of user private data.
- Financial harm to countries.
- Sharing of political,
- military information by attacker

2. LITERATURE SURVEY

1 U. Fiore, F. Palmieri, A. Castiglione, and A. D. Santis, "**Network anomaly detection with the restricted Boltzmann machine". [1]** With the rapid growth and the increasing complexity of network infrastructures and the evolution of attacks, identifying and preventing network abuses is getting more and more strategic to ensure an adequate degree of protection from both external and internal menaces. In this scenario many techniques are emerging for inspecting network traffic and discriminating between anomalous and normal behaviors to detect undesired or suspicious activities. Unfortunately, the concept of normal or abnormal network behavior depends on several factors and its recognition requires the availability of a model aiming at characterizing current behavior, based on a statistical idealization of past events. There are two main challenges when generating the training data needed for effective modeling. First, network traffic is very complex and unpredictable, and second, the model is subject to changes over time, since anomalies are continuously evolving.

2 M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, **"Data-stream based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study". [2]** As advanced metering infrastructure (AMI) is responsible for collecting, measuring, and analyzing energy usage data, as well as transmitting this information from a smart meter to a data concentrator and then to a headed system in the utility side, the security of AMI is of great concern in the deployment of smart grid. In this paper, we analyze the possibility of using data stream mining for enhancing the security of AMI through an intrusion detection system (IDS), which is a second line of defense after the primary security methods of encryption, authentication, authorization, etc. We propose a realistic and reliable IDS architecture for the whole AMI system, which consists of individual IDSs for three different levels of AMI's components: smart meter, data concentrator, and AMI headed.

3 Bassam Sayed, Issa Traor´e, Isaac Woungang, and Mohammad S. Obaidat, **"Biometric Authentication Using Mouse, Gesture Dynamics."[3]** The mouse dynamics biometric is a behavioral biometric technology that extracts and analyzes the movement characteristics of the mouse input device when a computer user interacts with a graphical user interface for identification purposes. Most of the existing studies on mouse dynamics analysis have targeted primarily continuous authentication or user re-authentication for which promising results have been achieved. Static authentication (at login time) using mouse dynamics, however, appears to face some challenges due to the limited amount of data that can reasonably be captured during such a process. In this paper, we present a new mouse dynamics analysis framework that uses mouse gesture dynamics for static authentication. The captured gestures are analyzed using a learning vector quantization neural network classifier.

4 S. C. Arseni, E. C. Popovici, L. A. Stancu, O. G. Guta, and S. V. Halunga, **"Securing an alerting subsystem for a keystroke-based user identification system" [4]** Our keystroke-based user identification system represents a minimal implementation of a software system that can be used for continuous authentication of users, based on their keystroke dynamics. This paper brings into evidence the role of an alerting subsystem as a part of the software system mentioned above. Also, the paper presents a basic implementation of such a subsystem, based on the existing Syslog protocol, and a combined method for securing the protocol.

5 G. M. Amdahl and Pankoo Kim, **"Validity of the single processor approach to achieving large scale computing capabilities" [5]** For over a decade prophets have voiced the contention that the organization of a single computer has reached its limits and that truly significant advances can be made only by interconnection of a multiplicity of computers in such a manner as to permit cooperative solution. Variously the proper direction has been pointed out as general purpose computers with a generalized interconnection of memories, or as specialized computers with geometrically related memory interconnections and controlled by one or more instruction streams.

2.1 Problem Statement

Security has been one of the serious problems in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously to authenticate users. To solve this issue we propose a security system, named Internal Intrusion Detection and Protection System (IIDPS), which detects user's malicious behaviors launched toward a system.

2.2 Goals And Objective

- To implement a system for accuracy of detecting suspicious user is efficient than existing system List Item
- An Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors of users.
- Although other systems consume longer time for data analysis than the IIDPS does.
- Proposed system can also detect malicious behaviors for systems employing GUI interfaces.

2.3 Existing System

Networked control system using wireless communication networks, the modeling and design of a topology consisting of plant, controller and intermediate network systems were studied in, where the topology builds on the concept of the Wireless Control Network (WCN) architecture (for more details on the WCN, see related references listed in).

2.4 Proposed System

The Proposed system offer a security system, named Internal Intrusion Detection and Protection System (IIDPS), that detects malicious behaviors launched toward a system at SC level. The IIDPS 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 in a very user's log file for the user. The user's rhetorical options outlined as associate SC pattern of times showing in a very user's submitted SC sequence however seldom getting used by different users, are retrieved from the user's laptop usage history. The system must study the SCs generated and also the SC-patterns created by these commands so the IIDPS will find those malicious behaviors issued by them then forestall the protected system from being attacked.

3. SYSTEM ARCHITECTURE

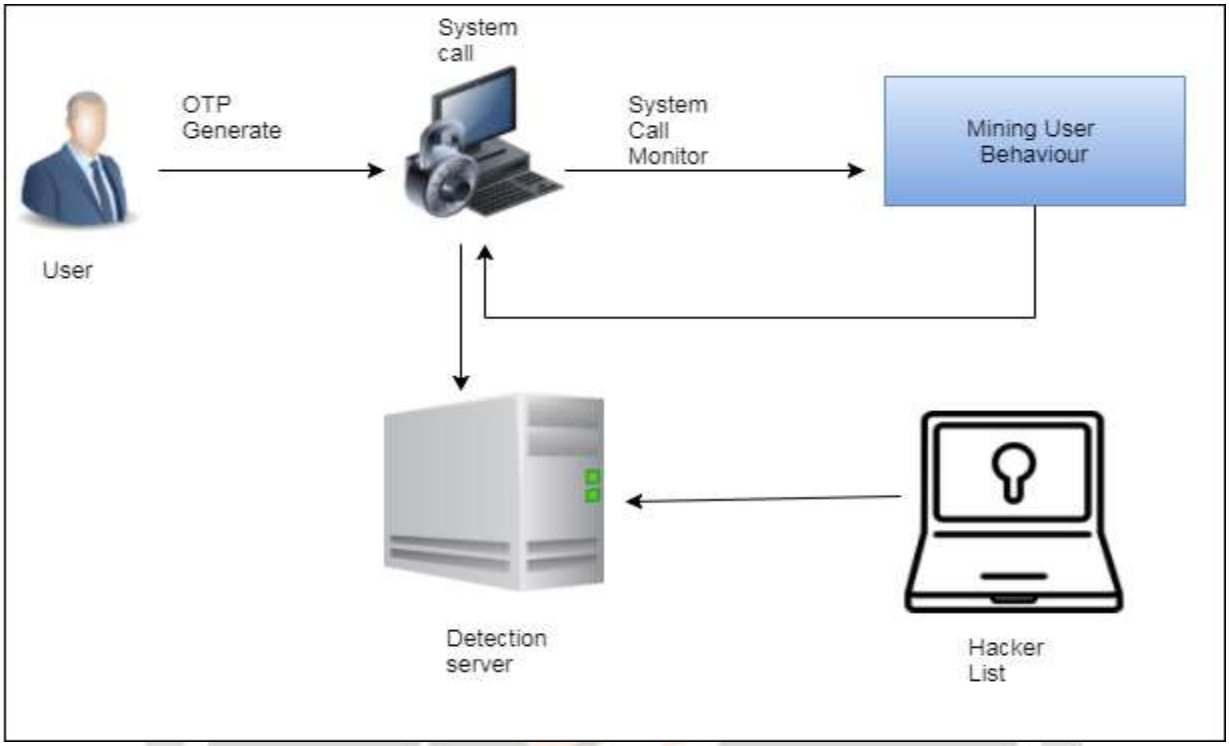

Fig. System Architecture

3.1 Data Flow Diagram

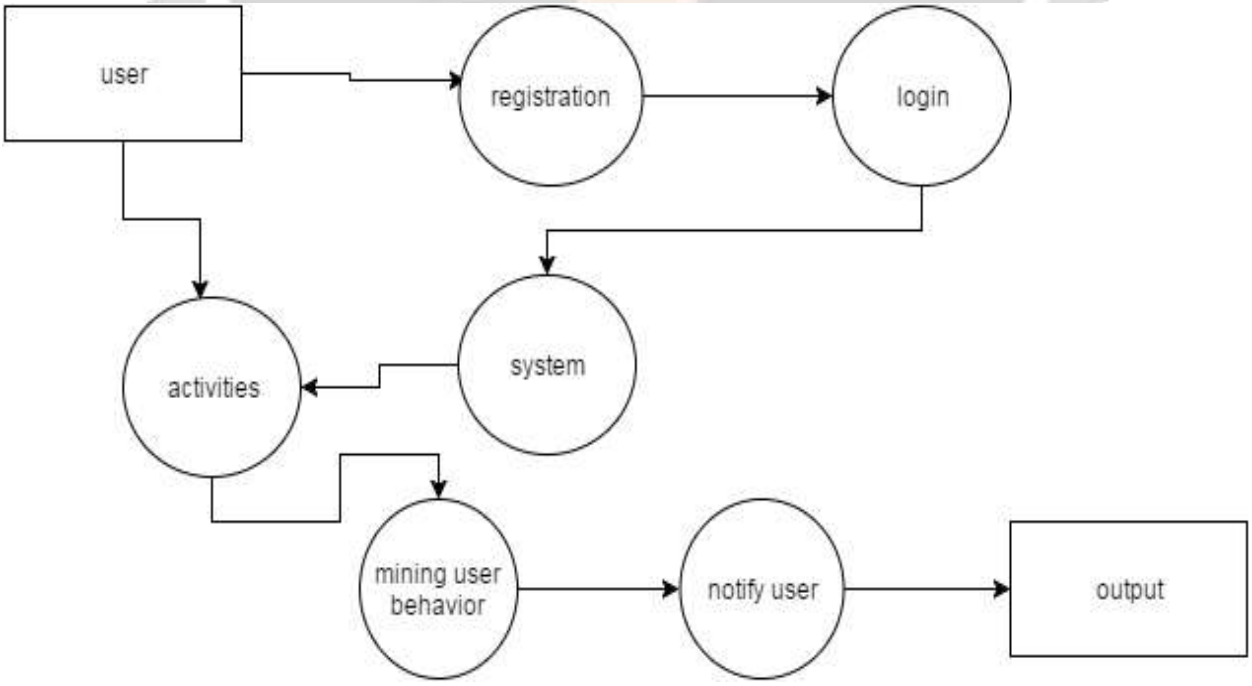

Fig. DataFlow Digram

3.2 Mathematical Model

Drive the mathematical model.

Let S be the j System as the final set

S = fU,Fr,G,A,Fg

Let U be the set of Users where,

S = fUg

U =fU1, U2, U3, U4:::::::j Ug

where, U1=user1.

U2=user2.

Let Fr be the set of Frame where,

S = fFrg

Fr = fFr1, Fr2, Fr3:::::j Frg

where, Fr1=Frame1

Fr2=Frame2

Let G be the set of Gesture where,

S={G}

G = fG1, G2, G3:::::j Gg

Let A be the set of Algorithm where,

S = fAg

A = fA1, A2, A3:::::j Ag

Identify the functions as ?F

S = fFg

F = fF1 (), F2(), F3(), F4(), F5(), F6(), F7(),F8(),F9()g

F1 (S) = Grab Image

F2 (S) = define gesture

F3 (S) = Grey Scale

F4 (S) = Threshold

F5 (S) = Bluring

F6 (S) =Image substraction

F7 (S) =Gesture Detection

F8 (S) =Add Product

F9 (S) =Manage Product

Deliver:-

Deliver the accurate virtual cloth fitting experience.

Decrease:-

Decreased the drawbacks of previous system.

4. CONCLUSION

The IIDPS (Internal Intrusion Detection and Protection System) employs data processing and rhetorical techniques to spot the user activity patterns for a user. The time that a habitual behavior pattern seems within the user's log file is counted, the foremost usually used patterns are filtered out, and then a user's profile is established. By distinctive a user's behavior patterns as his/her pc usage habits from the user's current input, the IIDPS resist suspected attackers. The long run work of business executive attack detection analysis is going to be concerning aggregation the important knowledge so as to check general solutions and models. It's onerous to gather knowledge from traditional users in many alternative environments. It's particularly onerous to amass real knowledge from a masker or traitor whereas activity their malicious actions. whether or not such knowledge were obtainable, it's a lot of possible to be out of reach and controlled below the foundations of proof, instead of being a supply of valuable info for analysis functions.

5. ACKNOWLEDGEMENT

I would like to thanks to my project guide **Prof. P.S.Gholap** who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work. To develop an Internal Intrusion Detection and Protection System that accurately updates databases according to the weights of goods and maintains transparency in the system and prevents forgery and exploitation of masses caused by consumer.

6. REFERENCES

[1]. B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2, pp. 262–274, Jun. 2013.

[2]. U. Fiore, F. Palmieri, A. Castiglione, and A. D. Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing*,vol. 122, pp. 13–23, Dec. 2013.

[3]. H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation based malware behavioral concise signature generation," *Inf. Commun. Technol.*, vol. 7804, pp. 271–284, 2013.

[4]. S. C. Arseni, E. C. Popovici, L. A. Stancu, O. G. Guta, and S. V. Halunga, "Securing an alerting subsystem for a keystroke-based user identification system," in *Proc. Int. Conf. Commun.*, Bucharest, Romania, 2014, pp. 1–4.

BIOGRAPHIES

	**Mali Rohini** She is currently learning BE degree in Computer Engineering from Pune University, Her research interested include An Internal Intrusion Detection and Protection System using Data Mining and Forensic Techniques.
	**Shedge Prajvaleeta** She is currently learning BE degree in Computer Engineering from Pune University, Her research interested include An Internal Intrusion Detection and Protection System using Data Mining and Forensic Techniques.
	**Unde Shital** She is currently learning BE degree in Computer Engineering from Pune University, Her research interested include An Internal Intrusion Detection and Protection System using Data Mining and Forensic Techniques.