International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - I **ISSN (Online): 2454- 1966**

Research Manuscript Title

IMPLEMENTATION OF IMPROVED APRIORI ALGORITHM IN INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM

Vijay K, Ranjith Kumar R, Saravanan M, Veni Devi G (AP-IT)

KCG College of Technology, Chennai, India.

E-Mail: kvijay88859@gmail.com, ranjithviru219@gmail.com, saravana11.tvt@gmail.com, venidevig@gmail.com

March – 2016

www.istpublications.com

International Journal of Future Innovative Science and Engineering Research (IJFISER), Volume - 2, Issue – I,
ISSN (Online): 2454- 1966 www.istpublications.com.

IMPLEMENTATION OF IMPROVED APRIORI ALGORITHM IN INTERNAL INTRUSION DETECTION AND PROTECTION SYSTEM

Vijay K, Ranjith Kumar R, Saravanan M, Veni Devi G (AP-IT)
KCG College of Technology, Chennai, India.
E-Mail: kvijay88859@gmail.com, ranjithviru219@gmail.com,
saravana11.tvt@gmail.com, venidevig@gmail.com

ABSTRACT

Most of the computer systems in the organizations use user IDs and passwords as the entry gateway to authenticate the users. But somehow they share or give their credentials to their coworkers for their work and request them to aid co-tasks, thereby losing their security of their credentials and making it as the one of the entry points for an attack. Intruders are basically of two categories. First thing is the external intruder. They are those who are the unauthorized users of the machines they attack and the next are the internal intruders who are those, who have the permission to access and work on the system, but will not have access to some portions of the system and they are hard to find and detect because most of the intrusion detection systems and firewalls can identify and isolate malicious behaviors from the outside the system only. Therefore a security system called the Internal Intrusion Detection and the Protection System referred to as (IIDPS) [1] is made to find and detect the insider who attacked the system and also to keep track of user's habit and finally to determine whether a valid user or not by comparing the current behaviors with the patterns collected and stored in the server before.

Keywords: Data mining, malicious behavior, user habits, intruder, security.

I. Introduction

Data Mining [4] is basically a concept of extracting or mining away the knowledge or the information needed from the large block-sets of data. Data mining is one of the way for identifying or to find the the intensive knowledge and information needed for use from those large amounts of data that is stored either in the databases, data warehouses, or the other repositories. Its trust and capacity is to discover valuable data efficiently, non-frequent information from those large databases. But it is certainly sometimes vulnerable to the wrong use of it. So, there might be some confusion among data mining and privacy. Basically, the mining process [8] will be done on this for effectively analyzing and obtaining the results. Privacy [5] basically refers to extraction of sensitive information using data mining. There is an alarming concern about the privacy of the individual users. Each individual has to control their information on their own. The general issues are the usage of other person's credentials or their information. Intrusion detection [6] is a research area where mining algorithms are used and analyzed for the effective detection of and protection for the individual's privacy concern and a brief can be found about it on the guide to IIDPS [7]. The Apriori Algorithm is an effective and suitable algorithm for mining the frequent item-sets for boolean association rules. There are two key concepts which are as follows. 1) The items must have minimum support. 2) The subset contained in the frequent item-set should be frequent.

Some of the possible threats to security are listed below.

1) *Risk* - Due to the malfunction of the hardware or due to the incomplete design or due to the incorrect software design because of which there may be an exposure of the information or the data or there may be some violation.

2) *Vulnerability* - Some known or suspected flaw because of which the hardware or software that is being used or the operation of a system that exposes the system to an accidental disclosure.

3) *Attack* – After the execution of a plan., a threat is carried out as a result

4) *Penetration* - A successful attack or a successful intruder one who can obtain the unauthorized access as a result to those files and programs to control the state of a computer system.

Intrusion detection systems (IDS) are basically focused on -

1) Identifying possible activities of the user and the system.
2) Gaining information about them.
3) Analyzing the vulnerability.
4) Assessing the file contents and the integrity of the system.
5) Recognizing malicious activities and patterns that are deviating.
6) Giving an alert to the administrator.

In addition, organizations use it generally for things like -

1) Identifying issues and the problems associated with that.
2) Analyzing the threats.
3) Following the security policies.

II. Related Work

Computer forensics [11] science views computer systems in order to identify, preserve, recover, analyze and present facts and opinions on information collected. It analyzes about the attackers and their behaviors like spreading some computer viruses, some malwares and some malicious codes. Most intrusion detection techniques focus on how to find malicious network behaviours [9] , [10] It means that, from synthetically generated log files, these traces or patterns of misuse can be more accurately reproduced. when an unauthorized user logs in to a system with a valid user ID and password.
Mining of frequent item-sets is an important part in the association mining to discover the frequent items from the list of item-set in the database. It is important to find the interesting patterns from datasets, such as the association, from the episodes, from the classifier, from the clustering and from the correlation etc. [12] Till now, there are so many algorithms to find out the frequent item-sets. But they can be grouped together only into two classes. They are 1) Ccandidate generation is the first class 2) Pattern growth is the second class. Apriori [13],[14] is like a subset of the candidate generation approach. It basically generates the candidate item-sets of length (k+1). It is based on the frequent item-sets of length (k). The item-set frequency can also be done by counting their occurrences during the transactions. Then at last in 2000,the Pattern growth was proposed by Han where he did some useful work about the FP tree.

III. Related details

This IIDPS generally uses two techniques to find the malicious behavior of the user who uses or accesses the account. The first one is basically like the physical entities. So many physical entities will be evaluated to find out about the malicious behavior. The physical entities such as finding where the user is accessing it and what system has been used frequently that would have been recorded before. So with that recorded information the behavior will be evaluated to find the data of who the intruder is.
The few characteristics of the physical entities with which the intruder can be traced out are –

1) By finding the physical location of the intruder.
2) By identifying the ip address of the system.

Next method is to find out the malicious behavior with the help of user's habits. The user who is accessing the account will have certain characteristics and these things are compared with those that are recorded in the server. From the result after comparing with the characteristics that are in the server, the malicious behavior can be obtained and the same can be reported to the admin as an alert or by mail.
The few characteristics of the user habitual entities with which the intruder can be traced out are

1) With the users preferences
2) A simple calculation.
3) OTP.

So by using few combinations of the above, Security points are made, and the originality of the user can be found. If there is some unusual behavior found after the comparison, then the admin will be intimated from this. So, the admin has the right to stop the access after identifying the malicious behavior. In case if the same is done across in an organization then the admin can ask the user whether to grant or stop the access. In the other case if it's a college the admin can directly stop the access after knowing that malicious behavior of the user who tries to access the system.

IV. The Improved Apriori Algorithm

The following is an algorithm for finding the frequent item set using the improved apriori algorithm.[15]
Input: transaction database D; min-sup.
Output: the set of Frequent L in the database D.
(1)min-sup-count=min-sup*|D|
(2)L1-candidates=find all one itemsets(D) //Scan D and produce L1-candidates
(3)L1={<X1,TID-set(X1)> L1-candidates |sup-count&'()-sup-count}
(4)for (k=2; Lk-1#*+,--.!/0!1
(5){for each k-itemset (xi,TID-set(xi) Lk-1 do
(6) for each k-itemset (xj,TID-set(xj) Lk-1 do
(7) if (xi[1]=xj[1])!(x i[2]=xj[2])!…!(xi[k-2]=xj[k-2] then
(8){Lk-candidates.Xk= Xi* Xj;
(9) Lk-candidates.TID-set(Xk) = TID-set(Xi) 234-set(Xj) }}
(10) for each k-itemset<Xk,TID(Xk)> Lk-candidates do
(11) sup-count=|TID-set|
(12)Lk={<Xk,TID-set(Xk)>Lk-candidates|sup-count&'()-sup-count}}
(13) set-count=Lk.item-count
(14)return L="kLk; [16]

Transactions in a database of D=10

TID	Items
T1	It1,It2,tI4
T2	It2,It5
T3	It2,It3
T4	It1,It2,It5
T5	It1,It2
T6	It2,It3
T7	It1,It3
T8	It1,It2,It3,It4
T9	It1,It2,It3
T10	It1,It4

Table 1. D of 10 Transactions

1)Scan D for count of each candidate.

Item Set	Support Count
It1	7
It2	8
It3	4
It4	3
It5	2

Table 2. Generation of C1

2)Support count of the candidate-set is then compared with that of the minimum support. Suppose that the minimum transaction support count required is 2.

Item Set	Support Count
It1	7
It2	8

It3	4
It4	3
It5	2

Table 3. Generation of L1

3)Generate C2 candidates from L1 and scan D for count of each candidate.

Item Set	Support Count
It1,It2	5
It1,It3	3
It1,It4	3
It1,It5	1
It2,It3	4
It2,It4	2
It2,It5	1
It3,It4	1
1t3,It5	0
It4,It5	0

Table 4. Generation of C2

4)Compare candidate support count with minimum support.
L2 is determined.Then D2 was determined from L2.

Item Set	Support Count
It1,It2	5
It1,It3	3
It1,It4	3
It2,It3	4
It2,It4	2

Table 5. Generation of L2

TID	Items
T1	It1,It2,It4
T4	It1,It2,It5
T8	It1,It2,It3,It4
T9	It1,It2,It3

Table 6. D2(Updated Table)

4) Generate C3 candidates from L2 and scan D2 for count of each candidate..

Items	Support Count
It1,It2,It4	2
It1,It2,It5	1
It1,It2,It3,It4	1
It1,It2,It3	2

Table 7. Generation of C3

Items	Support Count
It1,It2,It4	2
It1,It2,It3	2

Table 8. C3 (Updated Table)

6) Compare candidate support count with minsup.
The transactions in D2 are scanned in order to determine L3.

Items	Support Count
It1,It2,It4	2
It1,It2,It3	2

Table 9.Generation of L3

7) The algorithm uses L3 to generate a candidate set of 4-itemsets, C4.

TID	Items
T8	It1,It2,It3,It4

Table 10. Generation of D3

V. Proposed Work

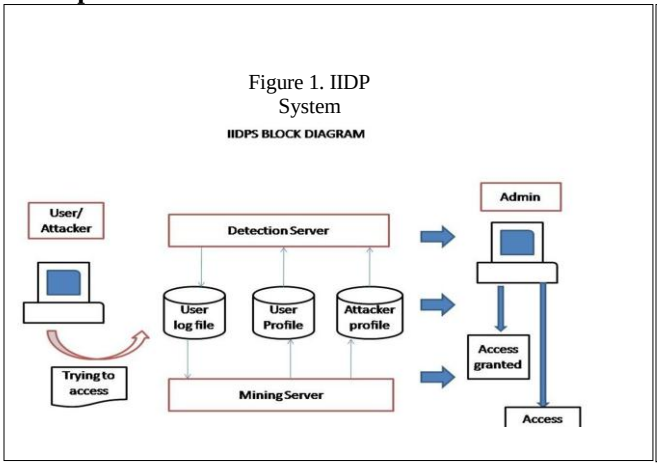


Figure 1. IIDP System

In this section, we have introduced the IIDPS system and the components of the IIDPS which are described in detail. An algorithm was also presented for generating a user habit file and detecting an internal intruder. The IIDPS system as in Figure1, consists of a mining server, a detection server and three repositories such as user log file repository, user profile repository and an attacker profile repository. So when a user/attacker tries to access the system, the IIDPS will check if it is a valid user by communicating with the admin. The admin after validating has the power to either grant the access to the user or can revoke the access from the user. By this way, the malicious behaviour if present can be found out with the help of the system.

Support: It is defined as rate of occurrence of an itemset in a transaction database.

$$S(I1 \rightarrow I2) = \frac{Tn(I1, I2)}{\mathrm{Tt}}$$

Where S is Support, Tn denotes number of transactions containing both item1 (I1) and item2(I2) . Tt denotes total number of transactions.

Confidence: For all transactions, it defines the ratio of data items which contains Y in the items that contains X.

$$C(I1 \rightarrow I2) = \frac{Tn(I1, I2)}{\mathrm{T(I1)}}$$

Where C is Confidence , Tn denotes number of transactions containing both item1(I1) and item2(I2). T(I1) denotes number of transactions containing item1 (I1).

VI. Implementation

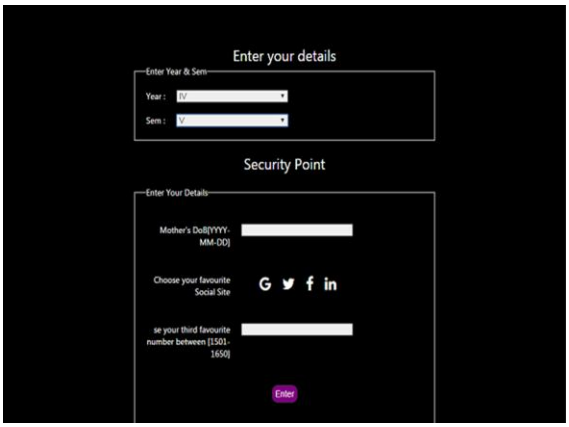
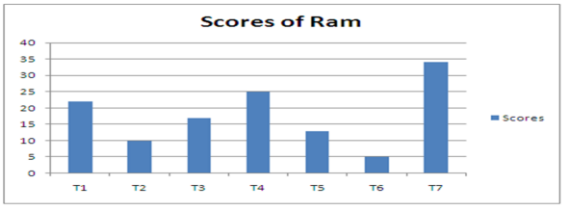


Figure 2. Security point check

The IIDPS system is implemented for an aptitude test system for finding whether the real user of the system is taking up the test. After that, their performance is calculated. The Figure 2, shows the security point which is used to check whether the user is real or not. The frequent item-set is generated after this which is shown in the Figure3, i.e. frequent item-set generation, which is used to monitor the students overall materials that was used by the students.

After that, the staff can login and monitor individual students performance as in figure 4 or can monitor the overall performance. A Report can be generated based on the staffs need either semester wise or year wise, to monitor the students performance.

Figure 4. Scores of Ram



VII. Conclusion and Future Work

In this paper, we have proposed a system which is called the Internal Intrusion Detection and Protection System(IIDPS). The user's preferences are recorded and compared every time when he logs in to the account. So based on the usage profile and the patterns the IIDPS restricts the intruder. In today's world, internal intrusion detection is one of the major topics in which the research is still going on for its effective development. It can be extended to protect the system even at a higher level by using one of the following two ways. First one is that the IIDPS system can be still improvised by introducing new concepts and thereby protecting it from intrusion efficiently. Second one is by extending the system by incorporating recent technologies such as finger print technology or a face detector technology to easily identify the user, thereby avoiding the malicious activity and to improve the IIDPS's performance. There are so many researches taking place in this field and a suitable one can be included to effectively develop the IDP system to protect the system.

References

[1] Fang-Yie Leu, Kun-Lin Tsai, Member, IEEE, Yi-Ting Hsiao, and Chao-Tung Yang "An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques " IEEE 2015.

[2] Akshita Bhandari Ashutosh Gupta Debasis Das" Improvised Apriori Algorithm using Frequent Pattern Tree for Real Time Applications" ICICT 2014. http://arxiv.`org/abs/1411.6224

[3] Sakshi Aggarwal1, Ritu Sindhu "An Approach of Improvisation in Efficiency of Apriori Algorithm" PeerJpreprints 2015.

[4] J. Han and Kamber, "Data Mining: Concepts and Techniques", 2nd ed., The Morgan Kaufmann Series in Data Management Systems, Jim Gray,Series Editor 2006.

[5] M. B. Malik, M. A. Ghazi and R. Ali, "Privacy Preserving Data MiningTechniques: Current Scenario and Future Prospects", in Proceedings of Third International Conference on Computer and Communication Technology ,IEEE 2012.

[6] Sheetal Thakare1 ,Pankaj Ingle2, Dr. B.B. Meshram, "Intrusion Detection System the Survey of Information Security", International Journal of Emerging Technology and Advanced Engineering , Volume 4 , Issue 8, August 2012.

[7] Guide to Intrusion Detection and Prevention System, NIST, Technology Administration US Department of Commerce.

[8] Pingshui WANG "Survey on Privacy Preserving Data Mining" International Journal of Digital Content Technology and Its Applications.Volume 4, Number 9, December 2010.

[9] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious Nodes Identification Scheme in Network-Coding-Based Peer-to-Peer Streaming," in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1–5.

[10] Z. A. Baig, "Pattern Recognition for Detecting Distributed Node Exhaustion Attacks in Wireless Sensor Networks," Compute. Commun., Vol. 34, No. 3,pp. 468–484, Mar. 2011.

[11] Z. B. Hu, J. Su, and V. P. Shirochin "An Intelligent Lightweight Intrusion Detection System With Forensics Technique," in Proc. IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst.: Technol. Appl., Dortmund, Germany, 2007, pp. 647–651.

[12].Rao S, Gupta R, Implementing Improved Algorithm Over Apriori Data Mining Association Rule Algorithm, International Journal of Computer Science And Technology, pp. 489-493, Mar. 2012.

[13]. Srikant R, Fast Algorithms for Mining Association Rules and Sequential Patterns, University of Wisconsin, 1996.

[14] Pratibha Mandave, Megha Mane, Prof. Sharada Patil, "Data mining using Association Rule Based on Apriori Algorithm and Improved Approach With Illustration", International Journal of Latest Trends in Engineering and Technology (IJLTET), November 2013

[15] Xiang Fang, "An Improved Apriori Algorithm on the Frequent Item set", International Conference on Education Technology and Information System (ICETIS 2013)

[16] SurajP. Patil1, U. M. Patil2 and Sonali Borse ,"The Novel Approach for Improving Apriori Algorithm for Mining Association Rule", Proceedings of "National Conference on Emerging Trends in Computer Technology (NCETCT-2012)"Held at R.C.Patel Institute of Technology, Shirpur, Dist. Dhule, Maharashtra, India. April 21, 2012.