A Secure Approach for Intruder Detection using Backtracking

Ms. Sushma Sukesh Shetty[1], Ms. Swathi[2], Ms. Jayapadmini Kanchan[3]

[1,2]BE Student, Department of Information Science and Engineering, Sahyadri College of Engineering and Management, Karnataka, India
[3]Assistant Professor, Department of Information Science and Engineering, Sahyadri College of Engineering and Management, Adyar, Mangaluru

---***---

Abstract - *Intrusion is one sort of attack where behaviour of an external or internal node(s) with maligns intent, which aims to affect other benign nodes in the network. One of the objective of the intruder is to stay undetected for whatever length of time that conceivable so they can proceed with their malevolent action undisturbed. An intruder can be a malicious hacker, former employee or one of the thousands of third party connections organizations. Intruder detection is done by analyzing the traffic passing on the entire subnet and matches the traffic that is passed on the subnets to the library of known attacks. Once the attack is distinguished or the abnormal behaviour is sensed the alert can be sent to the administrator. It identifies the activities that could be a precursor of more genuine attacks. The intruder attempts to gain unauthorized access to the system and behaves like a spoof. To detect the intruder we make use of the backtracking method which helps in tracking the previous transactions and identifies the intruder*

Key Words: Intruder, Backtracking, Attack, Network Security, Unauthorized access

1. INTRODUCTION

In the realm of expanding improvement over the web arrange which makes it hard to distinguish the dangers for PC security. A standout amongst the best answers for the referenced issue is Intrusion Detection System (IDS). It is a tool or a mechanism which can perceive attacks endeavour by breaking down the action of system. To take a shot at things that depend on system we utilize organize security. System Security is one of the most significant factor to think about when working over the web, LAN or other technique, regardless of how little or enormous your business is. It deals with the policies and practices adopted to prevent, and then monitor unauthorized access, misuse, modification or denial of computer network.

An Effective Network Security gives access to the system and targets different dangers and prevents them from entering or spreading to your system. It joins the different numerous layers of resistances at the edge and in the system. Each Network Security layer utilizes strategies and controls approved client access arrange sources however noxious on-screen characters are obstructed from performing parcel of endeavours and dangers. A decent system security framework helps business in lessening the danger of falling victim of data theft and harm.

Network Security utilizes Encryption algorithms which are ordinarily used in computer communications. Usually they provide secure transfers. If an algorithm is involved in a transfer, the file is first translated into a seemingly meaningless cipher text and then sent in this configuration; the receiving computer uses a key to translate the cipher into its original form. So if the message or record is caught before it achieves the accepting computer then it is in an unusable (or encrypted) structure. We utilize the AES algorithm for this methodology.

Network Security has various advantages. It helps in protecting personal data of customers which is existing on network. It provides protection of information that is shared between computers on the network and provides various dimensions of access when various computers attached to a network, here might be a few computers that may have more noteworthy access to data than others. Private systems can be given the best assurance from outside attacks is by shutting them off from web.

This paper presents mainly on detecting the intruder who causes intrusion attacks. When sender sends a message it is received by the receiver through the IDS, which contains intermediate nodes which forwards the message to the receiver. The receiver checks if the message is sent from intruder or not by backtracking method. This process compares the nodes of predefined path table and transaction table, if there is any difference in one node key while comparison between the two tables is said that is intruder is detected.

2. RELATED WORK

Grzegorz Kolaczek et al. [1], has clarified Intrusion detection system characterized a significant and dynamic research zone for digital security. The job of Intrusion Detection System inside security engineering is to improve a security level by distinguishing proof of all malevolent and furthermore suspicious occasions that could be seen in PC or system framework. The objective of the examination performed was check of the abnormality discovery frameworks capacity to oppose this kind of attack. It utilizes

Clustering algorithm and Classification algorithm for its methodology. This paper displays the fundamental consequences of tests taken to explore presence of attack vector, which can utilize ill-disposed guides to cover genuine attacks from being distinguished by interruption identification frameworks. Yagnik A Rathod et al. [2], has clarified a methodology for interruption recognition framework for database the board framework. This methodology focus on security approaches for exchanges allowed with DBMS. Data is presently days consider as asset for any association and data is overseen by DBMS. Database overseer deals with all security arrangements and checking access to database. The methodology utilized in this paper is mark age algorithm, Automatic malevolent location algorithm. Whatever the yield of the mark age algorithm, will be contrasted and signature got from chronicled information. Yali Yuan et al. [3], has clarified the Two Layers Multi-class Detection (TLMD)method utilized together with the C5.0 technique and the Naive Bayes algorithm is proposed for versatile system interruption recognition, which improves the identification rate just as the false alarm rate. The test results demonstrate that the proposed TLMD strategy has a diminished false caution rate and a decent discovery rate dependent on the imbalanced dataset. In this paper, they have planned another two layers multi-class identification technique for improving the execution of system interruption detection.Wang Andi et al. [4], has clarified the inconsistency identification strategy for client conduct is utilized to identify the inside aggressors of database framework. They have utilized Discrete Time Markov Chain model to separate conduct highlights of an ordinary client and the recognized client and make an examination between them. In the event that the deviation of highlights is past edge, the recognized client conduct is made a decision as an oddity conduct. In light of the discovery of clients' surprising conduct, a DDOS attacks location framework has set up to break down clients' conduct. Drashti Nandasanaet al. [5], has clarified about the mark based methodology, which is characterized on job chain of command. jobs characterize the client and make the board simple. We have chipped away at substantial exchange groupings which are put away in profile table. It utilizes Intrusion location algorithm and Learning algorithm. This methodology deals with benefit right checking at trait level. The upside of this methodology is that identification procedure is quick and less upkeep diminishes extra room. Mohammed Talebi et al. [6], has clarified that the data assumes a critical job in associations. Customary instruments, for example, encryption, get to control, and confirmation can't give an abnormal state of certainty. So they proposed a novel kind of interruption location framework for distinguishing attacks in both database exchange level and client task level in a high-rate exchange preparing. Our model is isolated into two sections: identification strategy at exchange level and between exchange levels. Identification technique at exchange level depends on depicting the normal exchanges inside the database applications. This methodology utilizes the Data mining algorithm. This is additionally centered around abnormality identification and utilized information mining to discover reliance and grouping rules in where between exchange level is utilized. Mostafa Doroudian et al. [7], has clarified the information mining algorithm that catches the working extent of the clients. It removes visit thing sets as working extensions and furthermore clarified about Appriori algorithm that utilized for finding the continuous between exchange conditions. The principle approach of this paper is it can identify pernicious practices in both exchange and between exchange levels. For this reason, they proposed a location technique at exchange level, which depends on depicting the normal exchanges inside the database applications. Zegui Ying et al. [8], has clarified while acquiring data learning advantageously. This paper for the most part contemplates a circulated interruption location framework model and presents the impact of various information stockpiling modes on discovery of algorithm. At last, it advances diverse recognition algorithms as per distinctive capacity modes and improved plans went for conventional identification algorithm. Different modules of dispersed interruption recognition framework are conveyed on PCs and different modules are commonly sorted out on the guideline of chain of command and all modules are joined together to shape an interruption discovery framework. This paper presents the meaning of dispersed interruption location framework and examines identification algorithm utilized in this paper, including important segment investigation algorithm, bunching algorithm, choice tree algorithm and self-arranging trademark mapping algorithm first and after that advances improved discovery algorithm lastly dissects the relationship among information and the progression of setting up an ordinary conduct model went for databases in various division modes. Ci Chen et al. [9], has clarified about the class affiliation rule mining approach dependent on Genetic Network Programming(GNP) for distinguishing system interruption consolidating abuse identification and oddity location. The proposed methodology is an expansion of the interruption recognition approach utilizing GNP, so it can recognize and recognize ordinary, known interruption and obscure interruption. The reproduction result demonstrates that the identification rate is improved contrasted and customary interruption recognition approach so the known interruption and obscure interruption are recognized with high exactness. Yoseba K. Penya et al. [10], has clarified about Network Intrusion Detection Systems (NIDS) that have the test to forestall organize attacks and unapproved remote utilization of PCs. So as to accomplish this objective, NIDS as a rule pursue two unique methodologies. The first goes for recognizing prohibited utilization of the system and the second one focuses on discovering ill-conceived conduct. The principal technique achieves its objective by characterizing every single imaginable attack and the second by demonstrating the typical use to distinguish whatever does not fit on that marshal, this distinction has rendered the two options so far inconsistent. In past works we have introduced ESIDE-Depian, the principal naturally brought together abuse and irregularity locator. For this methodology it utilizes the Naive Bayes algorithm. This paper centers around the issues and diffculties that emerged in the joining procedure and the arrangements intended to conquer them. Weiming Hu et al. [11], has clarified about going for developing an interruption discovery approach with a low computational intricacy, a high identification rate, and a low false-alert rate, in this correspondence, we apply the AdaBoost algorithm to intrusion detection. The inspiration for applying the AdaBoost algorithm. In this algorithm choice stumps are feeble classiffers algorithm. Test results demonstrate that our algorithm has low computational multifaceted nature and blunder rates, as contrasted and algorithm s of higher computational intricacy, as tried on the benchmark test information. Jiong Zhang et al. [12], has clarified about proposing another methodical systems that apply Random Forest algorithm in abuse, irregularity, and half and half system based IDSs. In abuse identification, examples of interruptions are assembled consequently by RFA over preparing information. After that,intrusions are identified by coordinating system exercises against the examples. In abnormality discovery, novel interruptions are recognized by the exception location component of the RFA. In the wake of structure the examples of system benefits by this algorithm, exceptions identified with the examples are dictated by the anomaly location algorithm. The half and half location framework improves the identification execution by consolidating the benefits of the abuse and oddity recognition. We assess our methodologies over the Knowledge Discovery and Data Mining 1999 (KDD'99) dataset. The exploratory outcomes exhibit that the execution given by the proposed abuse approach is superior to the best KDD'99 resuls, contrasted with other revealed unsupervised oddity identification approaches, our abnormality location approach accomplishes higher discovery rate when the bogus positive rate is low and the displayed mixture framework can improve the general execution of the previously mentioned IDSs. Randy Smith et al. [13], has clarified about investigating NIDS avoidance through algorithmic multifaceted nature attacks. We present an exceptionally compelling attack against the Snort NIDS, and we give a commonsense algorithmic arrangement that effectively frustrates the attacks. This attack misuses the conduct of guideline coordinating, yielding assessment times that are up to 1.5 multiple times slower than that of kind hearted parcels. Our examination demonstrates that this attack is relevant to numerous guidelines in Snort's ruleset, rendering defenceless the large number of systems secured by it. Our countermeasure limits the investigation time to inside one request of greatness of favourable bundles. Here we utilize Backtracking algorithm. Trial results utilizing a live framework demonstrate that an assailant needs just 4.0 kbps of data transfer capacity to interminably incapacitate an unmodified NIDS, though all interruptions are identified when our countermeasure is utilized. Sriranjani Sitaraman et al. [14], has clarified about Existing instruments, as BackTracker, help the framework chairman backtrack from the location point, which is a document with suspicious substance, to conceivable section purposes of the interruption by giving a diagram containing reliance data between the different records and procedures that could be identified with the recognition point. We improve such backtracking procedures by logging certain extra parameters of the document framework amid ordinary tasks (ongoing) and looking at the logged data amid the investigation stage. Here we utilize the chart age algorithm. Furthermore, we use information stream examination inside the procedures identified with the interruption to prune undesirable ways from the reliance chart. This outcomes in noteworthy decrease in pursuit space, seek time, and false positives. We additionally examine the exertion required regarding extra room and inquiry time. Covera S. et al. [15], has clarified about foundation. Abnormality discovery is a key component of interruption identification in which bothers of ordinary conduct recommend the nearness of deliberately or unexpectedly incited attacks. The significant advantage of irregularity identification algorithms is their capacity to conceivably distinguish unanticipated attacks. In this paper we give best in class audit in the territory of curiosity location dependent on information mining strategies. Talked about is the different models adequacy and their particular deficiencies, just as the trouble of oddity location by and large. In directed abnormality identification, given o set of ordinary information to prepare on, and given another arrangement of test information, the objective is 10 decide if the test information is typical or atypical. Unsupervised irregularity identification is a variation of the established anomaly location issue. These algorithms can likewise be alluded to as irregularity discovery over uproarious information. The reason the algorithm must probably deal with clamour in the information is that we would and like to physically confirm that information contains no interruptions.

2. 1 ARCHITECTURE DIAGRAM

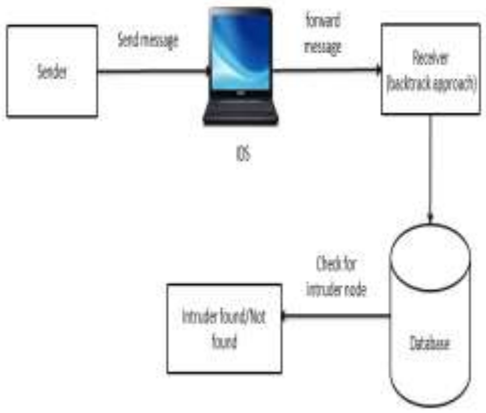

Fig -1: Architecture of Intruder Detection

The process of detection of intruder is as follows Fig-1 represents the architecture of intruder detection.

The Sender sends the message to receiver through the IDS. The receiver receives the message that is been forwarded by the IDS. The receiver needs to check whether the message is normal or intruded. This can be done by a backtrack approach. The receiver undergoes backtracking which fetches the details from the database which then compares the node key of the predefined path and the transaction table. To encrypt and decrypt the key we make use of a AES algorithm.

After the comparison between the keys of nodes of path table and keys of nodes of transaction table, in case if there is difference in any one of the node key then the intruder is found, else intruder is not found.

2.2 IMPLEMENTATION

The detection of the intruder is done by the backtracking method. The backtracking method consists of the following steps:

```
Step 1: Start
Step 2: Default key is maintained in an array
Step 3: Transaction key is maintained in another
        Array which may or may not contain
        an intruder key
Step 4: Then both the array values are
        Compared starting from the last index
        of the array
Step 5: Once the intruder key is found then
        the loop breaks
Step 6: The name of the intruder key is
        assigned to the label which displays
        the intruder name
Step 7: End the process
```

2.3 RESULT AND ANALYSIS

In this analysis, we get two cases, i.e. intruder found and intruder not found, which helps in the process of detection of the malicious activity going on within the network or not. We make use of the backtracking method which detects the intruder more accurately and alarms the person about the intruder being detected there itself. This approach improves the security within the network.

3. CONCLUSION

The project is developed with an objective in order to detect the intruder causing the intrusions. The aim is satisfied with help of Network Security techniques which will identify the intruder. It helps us to distinguish between the normal and intrusive events. In this paper a secure approach for intruder detection using backtracking method is shown. The receiver end undergoes the backtracking which compares the predefined path table and transaction table, where the backtracking starts from last transaction and then continues until the intruder is found, once the intruder is found the method is stopped and displays the intruder name. During the comparison if there is no difference of node keys in both the tables then no intruder is found. According to our experimental results the backtracking method detects the intruder more accurately and improves the security.

REFERENCES

1. Chunjie Zhou, Shuang Huang, N Xiong, Shuang-Hua Yang “Design and Analysis of Multimodel Based Anaomaly Intrusion Detection Systems in Industrial Process Algorithm”, IEEE Transactions on Systems, Man and Cybernetics, 2015

2. Arkadiusz Warzyński and Grzegorz Kołaczek “Intrusion Detection Systems Vulnerabilities on adversial examples”, IEEE Conferences, 2018

3. Yagnik A Rathod, Prof. M.B. Chaudhari, Prof. G.B. Jethava “Database Intrusion Detection by Transaction Signature”, IEEE Conferences 2018

4. Yali Yuan, Liuwei Huo, Dieter Hogrefe “Two Layers Multi-class Detection Method for Network Intrusion Detection System”, IEEE Symposium on Computers and Communication Conferences, 2017

5. Bi Meng, Wang Andi , Xu Jian , Zhou Fucai “DDOS Attack Detection System based on Analysis of Users Behaviors for Application Layer”, IEEE International Conference on Computational Science and Engineering and IEEE International Conference on Embedded and Ubiquitous Computing, 2017

6. Drashti Nandasana, Mr. Virendra Barot “A Framework for Data Intrusion Detection System”, IEEE International Conference on Global Trends in Signal Processing, Information Computing and Communication, 2016

7. Mostafa Doroudian, Narges Arastouie, Mohammad Talebi, Ali Reza Ghanbarian “Multilayered Database Intrusion Detection System for Detecting Malicious Behaviors in Big Data Transaction”, IEEE Conferences, 2015

8. [8] Mostafa Doroudian, Hamid Reza Shahriari “A Hybrid Approach for Database Intrusion Detection at Transaction and Intertransaction Levels”, IEEE Conference on Information and Knowledge Technology, May 28-30, 2014.

9. Diangang Wang, Zegui Ying, Hong Guo, Xiaoqiang Peng "Research and Design of A New Intrusion Detection System Model", IEEE Second International Conference on Computer Modeling and Simulation, 2010

10. Yunlu Gong, Shingo Mabu1, Ci Chen1, Yifei Wang and Kotaro Hirasawa "Intrusion Detection System Combining Misuse Detection and Anomaly Detection Using Genetic Network Programming", IEEE International Joint Conference August 18-21, 2009

11. Yoseba K. Penya, Pablo G. Bringas "Experiences on Designing and Integral Intrusion Detection System", IEEE 19th International Conference on Database and Expert Systems Application, 2008

12. Weiming Hu, Wei Hu and Steve Maybank "AdaBoost-Based Algorithm for Network Intrusion Detection", IEEE Transactions On Systems, Man and Cybernetics-Part B: Cybernetics, Vol. 38, No. 2, April, 2008

13. Jiong Zhang, Mohammad Zulkernine, and Anwar Haque "Random-Forests-Based Network Intrusion Detection Systems", IEEE Transactions on Systems, Man and Cybernetics-Part C:Applications and Reviews, Vol. 38, No. 5, September, 20088, No. 2, April, 2008

14. Randy Smith, Cristian Estan, Somesh Jha "Backtracking Algorithmic Complexity Attacks Against a NIDS", IEEE 22nd Annual Computer Security Applications Conference, 2006

15. Sriranjani Sitaraman and S. Venkatesan " Forensic Analysis of File System Intrusions using Improved Backtracking", IEEE Third International Conference on Information Assurance, 2005

16. Corvera S., Grau, AB, Andifla U., Dr. Universidad Yolitknica de Illadrid "Anomaly Detection Schemes In Network Intrusion Detection", IEEE International Conferences, 2004