IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

Host Based Intrusion Detection and Blocking Using B-Tree Approach

Pratviraj Singh Rathod, Swathi J Gowda, Supritha S, Vidya Bai S B, Mr. Sandeep K H

Dept. of Computer Science and Engineering, PESITM, Shivamogga, Karnataka, India

Dept. of Computer Science and Engineering, PESITM, Shivamogga, Karnataka, India

Dept. of Computer Science and Engineering, PESITM, Shivamogga, Karnataka, India

Dept. of Computer Science and Engineering, PESITM, Shivamogga, Karnataka, India

Assistant Professor, Dept. of Computer Science and Engineering, PESITM, Shivamogga, Karnataka, India

ABSTRACT: Intrusion detection is the act of determining and acknowledging to apprehensive movements addressed at computing as well as communication assets. Due to the dramatic increase in the number of attacks, and it has become the central point of information security. Intrusion detection system (IDS) auditors not only gathers data from a target system that should be secured, processes and correlates the gathered information, but also commence feedbacks when evidence of an intrusion is detected. In this paper, we designed and implemented a host-based intrusion detection system, which fuses two detection technologies. One of them is log file analysis technology. Another is Artificial Neural Network technology. Log file analysis is a path of misuse detection. Artificial Neural Network is an approach of anomaly detection. By combination of these two kinds of detection technologies, we have effectively implemented HIDS. Our implementation can enhance not only the efficiency but also accuracy of intrusion detection.

I. INTRODUCTION

An intrusion is the probable possibility of a prudent illegitimate pursuit to approach information, to wield information or unusable. After that, several techniques for detecting intrusions have been designed. The first intrusion detection system miniature was designed by Georgetown University Dorothy Denning and SR I / CSL's Peter Neumann. Intrusion detection system (IDS) auditors not only gathers data from a target system that should be secured, processes and correlates the gathered information, but also commence feedbacks when evidence of an intrusion is detected. There is three types if IDS based on their source of input. First is Host-based Intrusion Detection System (HIDS). Second is Network-based Intrusion Detection System (NIDS). Third is Hybrid Intrusion Detection System. Network- based intrusion detection system collects input data by monitoring network traffic. Host- based intrusion detection system assemble input dossier from the host it audits. Hybrid intrusion detection system assemble input dossier from both of network traffic as well as hosts it monitors. HIDS uses “Anomaly” detection as well as and “Misuse” detection techniques. Anomaly detection points to intrusions that can be disclosed based on divergent performance as well as usage of computer resources. In this paper not only we designed but also implemented a host-based intrusion detection system. This system uses pattern matching as well as artificial neural network as its detection methods. Initially, the HIDS uses log files as its primary sources of information. Then it can finally recognize various intrusions by using pre-decoding log file, decoding log file, and analysis log file. In the next step, based on artificial neural network analysis technology, the HIDS can determine intrusions by correlation with threshold. Experiment results presents that the HIDS can adequately boost not only the efficiency but also accuracy of intrusion detection. The rest of the paper we describes log analysis technology, artificial neural network analysis technology, the design and implementation of HIDS, gives some screenshot of experiment and conclusion. This paper introduces a novel approach to designing and implementing a HIDS utilizing log file analysis and ANNs. Unlike network- based IDS, which monitor traffic at the network perimeter, host-based systems operate directly within the host environment, allowing for deeper inspection of system activities, user interactions, and application behaviors. By focusing on the analysis of log files generated by various system components, our proposed HIDS gains insights into the intricacies of system behavior, enabling it to detect anomalous activities indicative of potential intrusions. as a rich source of information, containing records of system events, user actions, and network transactions.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

II. RELATED WORK

[1] In this paper an author proposed collaborative intrusion detection networks. It aims to improve the detection capability of an IDS node through collecting and learning useful information from other IDS nodes. In this paper. [2] an author explained the case of distributed intrusion detection systems running over P2P networks as well as proposed Indra, a distributed scheme. This is based on allocating information between trusted associates in a network. In this paper. [3]an author improved their proposed trust management model. It is done by maintaining the Dirichlet family of probability density functions in the trust management. [4]an author practiced a Bayesian approach to feedback aggregation. It was aiming to diminish not only the combined costs of missed detection but also false alarms. [5] an author proposed a feature extraction algorithm by using Factor Analysis as well as Support Vector Decision Function Ranking Method. [6]an author improved high false-alarm rates by using a combination of discriminative training and generic keywords. [7] an author uses a time-window method. The method allows us to generalize input, enabling us to recognize longer multi-packet attacks.

[8]an author proposed a novel approach for ANN-based IDS, FC-ANN. It enhances the detection precision for low frequent attacks and detection stability.

The behavior of computer system is recorded by Log files. It aims at recording the action of operating system as well as applications. Log file is widely used for system debugging, monitoring, and security detection. Log system is more crucial in intrusion detection. Log file analysis tool have become an essential appliances for daily inspection along with maintenance of the system running. Primarily, log analysis-based HIDS contains the: collection, predecoding, decoding, analysis of log file and report events.

III. PROPOSED SYSTEM

Our proposed system aims to develop a robust host-based intrusion detection system (HIDS) that leverages log file analysis and artificial neural networks (ANNs) for proactive threat detection and mitigation. Operating within the host environment, the system continuously monitors system activities, user interactions, and network transactions to identify potential intrusions. The system collects log files from various system components, including operating system logs, application logs, and network logs. These logs are preprocessed to extract relevant information such as timestamps, user IDs, system calls, and network communications. Preprocessing also involves normalization and filtering to ensure consistency and relevance of the data.

Utilizing the preprocessed log data, the system performs feature extraction to identify key attributes indicative of normal and anomalous behaviors. Features may include frequency of system calls, user login patterns, network traffic volume, and temporal correlations between events. The ANN architecture is designed to accommodate the extracted features as input nodes, with hidden layers facilitating the learning of complex patterns and relationships. Supervised learning algorithms, such as backpropagation, are employed to train the ANN model using labeled data representing both normal and intrusive activities.

Training involves iterative optimization of the network parameters to minimize prediction errors and enhance detection accuracy. The trained model is validated using separate validation datasets to assess its generalization ability and performance metrics such as accuracy, precision, recall, and F1-score.

In operational mode, the trained ANN model continuously analyzes real-time log data to detect suspicious activities indicative of potential intrusions. Incoming log entries are processed, and their features are fed into the ANN for classification as either normal or anomalous. Threshold-based techniques may be employed to determine the likelihood of intrusion based on the output probabilities from the ANN. The proposed system is designed to be scalable and adaptable to evolving cyber threats and system environments. The modular architecture allows for easy integration with existing security infrastructure and the incorporation of additional features or detection algorithms. Moreover, the ANN model can be periodically retrained using updated datasets to adapt to new attack patterns and improve detection efficacy over time. The proposed host-based intrusion detection system leveraging log file analysis and artificial neural networks offers an advanced and proactive approach to cybersecurity.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

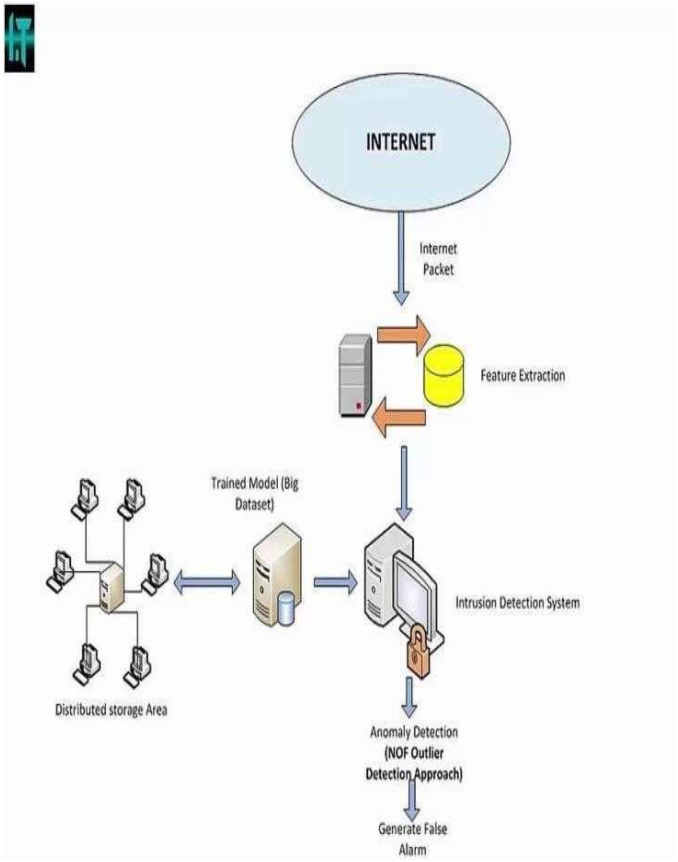

Fig 1: System Architecture.

IV. METHODOLOGY

The workflow of a host-based intrusion detection system (HIDS) with node creation for admin and user roles. Admins interact with the system through the admin interface, where they manage user roles and permissions, including node creation for individual users. Upon login, users access applications via the user interface, with their permissions managed by user node creation modules. The HIDS continuously monitors system activities and network traffic for anomalies, utilizing algorithms for anomaly detection and behavior analysis. Detected anomalies trigger alert generation, with alerts escalated as necessary based on severity. Administrators respond to alerts through mitigation actions, ensuring the security of the network and effective management of user access and permissions.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

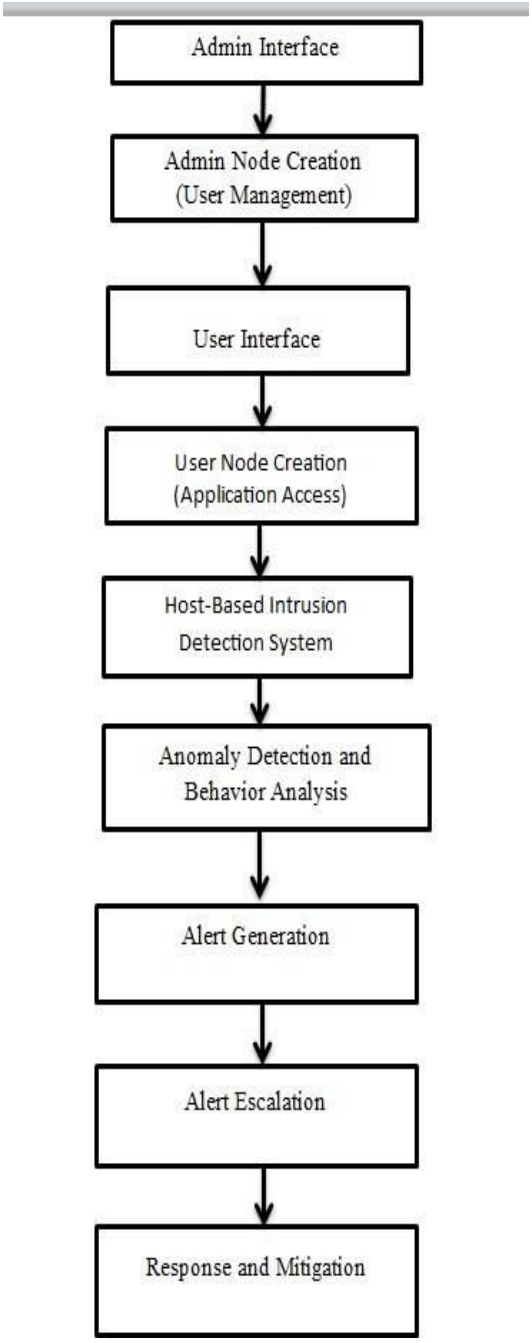

Fig 2 : Workflow of methods

V. RESULTS

The integration of MAC and IP authentication, coupled with OTP generation, significantly fortifies the host-based intrusion detection system's security framework. By implementing multi- factor authentication, the system ensures heightened accuracy in verifying user identities, thereby reducing the risk of unauthorized access. The inclusion of OTPs adds an additional layer of protection against potential threats like password theft or replay attacks. With these enhanced security measures in place, the system can effectively monitor user activities and system processes, promptly detecting and responding to suspicious behavior. Administrators receive timely alerts, enabling swift mitigation actions to be taken, ultimately bolstering the organization's cybersecurity defenses and minimizing the impact of potential security incidents.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

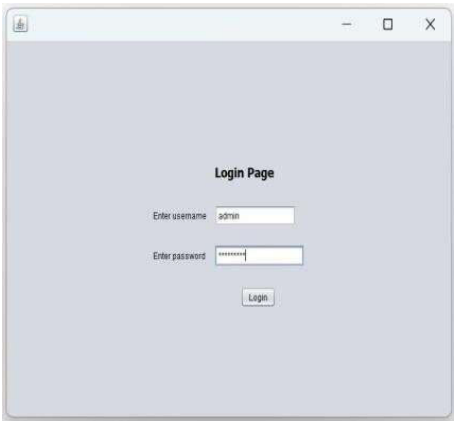

Fig:3 The Login Page

The Admin has to be loged in into the system by providing a proper username and password.

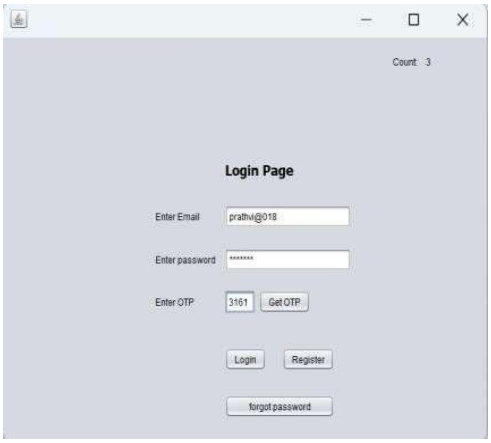

Fig:4 User Login Page

After the admin login user can register.

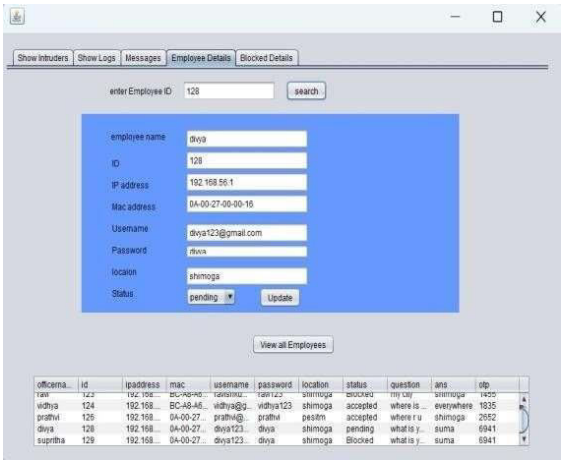

Fig:5 The Employee Detail

Here in this page it provides the complete details of the employees. And we will be having three options like

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

accept, pending and block buttons.

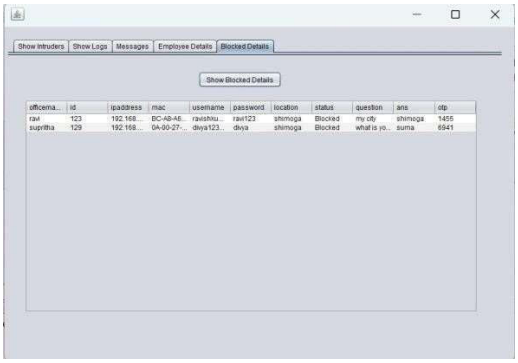

Fig:6 Blocked Details

In the blocked detail page contains the details of the blocked peoples and the timings, data, location, password, ip address and mac address.

The employees those who are doing suspicious activities like downloading the important files, it maybe related to bank details or confidential informations, those employees will be blocked immediately and the message will be sent to the user that you are blocked. And only admin can unblock them so that they can login again.

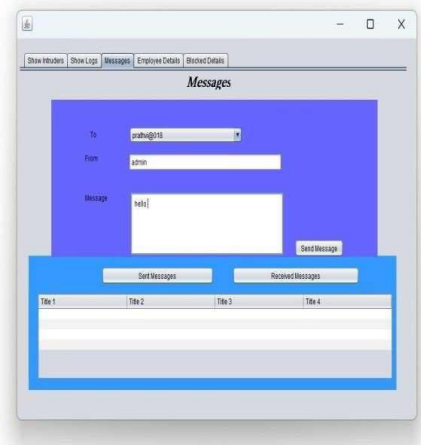

Fig: 7 Message Section

In this section the admin and the user can send or receive the message only to the authenticated user.

Fig: 8 Alert Message

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305051 |

If any of the user trying to login through the different system with the correct username and password then alert message will be sent to the admin with a beep sound so that they can take a proper action as soon as possible.

VI. FUTURE WORK

There are several avenues for enhancing the integrated system of MAC and IP authentication with OTP generation in a host-based intrusion detection system (HIDS). Future work could concentrate on refining anomaly detection algorithms to better identify sophisticated threats, integrating external threat intelligence feeds for real-time threat information, and incorporating user behavior analytics to detect insider threats. Additionally, optimizing system scalability and performance, implementing continuous security monitoring, and exploring user-friendly authentication methods would improve overall system effectiveness and user experience. Addressing these areas in future research and development efforts would further fortify the system's capabilities and resilience against evolving cyber threats.

REFERENCES

[1]. J.P Anderson, “Computer Security Threat Monitoring and Surveillance”, Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.
[2]. Dorothy Denning, “An Intrusion Detection Model”, IEEE Transactions on Software Engineering, February 1987, pp.2- 222.
[3]. G. Vigna and C. Kruegel, “Host-based Intrusion Detection Systems,” in The Handbook of Information Security, Volume III, John Wiley & Sons, December 2005.
[4]. Sandeep Kumar, Eugene H. Spaffor, “An application of Pattern Matching in Intrusion Detection”, Technical report 94-013,Purdue University, Department of computer sciences, March 1994.
[5]. Y.-S. Wu, B. Foo, Y. Mei, and S. Bagchi, “Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS,” Proceedings of ACSAC 2003, pp. 234– 244, 2003.
[6]. R. Janakiraman and M. Zhang, “Indra: a peer-to-peer approach to network intrusion detection and prevention,” Proceedings of the 12thIEEE International Workshops on Enabling Technologies, pp. 226– 231, 2003.
[7]. C.J. Fung, O. Baysal, J. Zhang, I. Aib, and R. Boutaba, “Trust Management for Host-Based Collaborative Intrusion Detection,” Proceedings of DSOM 2008, pp. 109–122, 2008.
[8]. C.J. Fung, J. Zhang, I. Aib, and R. Boutaba, “Robust and scalable trust management for collaborative intrusion detection,” Proceedings of the 2009 IFIP/IEEE International Symposium on Integrated NetworkManagement, pp. 33–40, 2009.
[9]. C.J. Fung, Q. Zhu, R. Boutaba, and T. Basar, “Bayesian Decision Aggregation in Collaborative Intrusion Detection Networks,” Proceedingsof NOMS 2010, pp. 349–356, 2010.
[10]. Y. Bai, and H. Kobayashi, “Intrusion Detection Systems: Technology and development,” Proceedings of AINA’ 03, 2003.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details