WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detection of Illegal Activity of an Employee in an Organisation

Ganesh G T[1], Harshit S[2], Abhishek C[3], Harshith M[4]

[1]Computer Science and Engineering Dayananda Sagar University, Bengaluru, India
[1]ganeshgtganeshgt@gmail.com, [2]harshithm21@gmail.com, [3]eng20cs0003@dsu.edu.in, [4]eng20cs0111@dsu.edu.in
DOI: https://doi.org/10.55248/gengpi.5.0524.1337

ABSTRACT

Insider cyber attacks represent a pervasive threat that continues to escalate in complexity and frequency, posing significant challenges for organizations globally. Perpetrated by individuals with privileged access to sensitive systems and information, insider attacks undermine the very foundations of trust and security within organizations. The ramifications of insider breaches extend far beyond mere financial losses, encompassing reputational damage, regulatory scrutiny, and erosion of customer confidence.

These insidious attacks manifest in various forms, ranging from the clandestine installation of malware on user devices to orchestrated campaigns targeting critical infrastructure and corporate networks. The insidious nature of insider attacks amplifies the risk of data corruption, theft, and manipulation, exposing organizations to unprecedented vulnerabilities and liabilities. Moreover, the collateral damage inflicted upon unsuspecting users, who may fall victim to identity theft and financial fraud, Our proposed approach represents a pivotal step towards fortifying the defenses against insider threats, empowering organizations to preemptively thwart malicious activities and safeguard critical assets. Through the seamless integration of machine learning techniques, organizations can augment their cybersecurity arsenal with proactive threat intelligence capabilities, enabling real-time detection and response to emerging threats.

Our system comprises two distinct servers: an original server housing genuine data and sensitive information, and a honeypot server strategically designed to entice potential attackers. The honeypot server serves as a decoy, containing dummy files intended to lure malicious insiders attempting to access unauthorized information. Meanwhile, as the attacker interacts with the honeypot server, the system discreetly sends alerts to the IT Administrator, enabling swift intervention and response to the security breach.

The core objective of our model is to establish a proactive defense mechanism against insider threats, thereby safeguarding the integrity and confidentiality of organizational data. By hosting both original and decoy servers, our system not only detects suspicious activities but also provides valuable insights into the methods and motivations of malicious insiders. Through comprehensive tracking and monitoring, we aim to enhance accountability and deterrence, ultimately fortifying the resilience of organizational systems against insider attacks.

In summary, our approach represents a pivotal advancement in combating insider threats by leveraging innovative technology and strategic deployment of decoy servers. By prioritizing early detection, swift intervention, and proactive mitigation, our model empowers organizations to mitigate risks, protect critical assets, and uphold the trust and integrity of their operations in an increasingly complex digital landscape.

INTRODUCTION

In contemporary organizational landscapes, the threat posed by insider cyber attacks looms large, necessitating vigilant measures to mitigate potential risks and safeguard critical assets. Insider threats, perpetrated by employees with privileged access to sensitive information systems, pose a formidable challenge to the security infrastructure of enterprises worldwide. The absence of robust monitoring protocols leaves unmonitored systems vulnerable to illicit activities, including data theft and unauthorized access, perpetrated by insiders exploiting their unrestricted access privileges.

In response to this pressing concern, our project endeavors to devise an innovative approach aimed at detecting and intercepting illegal activities perpetrated by insider employees within organizational systems. Central to our model is the recognition that traditional security measures often fall short in effectively mitigating the risks posed by insider threats. To address this gap, our proposed model not only focuses on the detection and prevention of insider attacks but also emphasizes the importance of tracking these activities back to their source.

At the heart of our system lies a dual-server architecture comprising an original server and a honeypot server strategically designed to lure potential attackers. The original server hosts critical sensitive data and authentic information vital to the organization's operations, while the honeypot server serves as a decoy, containing dummy files intended to entice and deceive malicious insiders. This simulated environment creates a bait-and-trap mechanism, enabling the identification and interception of insider threats in real-time.

The deployment of our model aims to fortify the resilience of organizational systems against insider attacks by providing administrators with actionable insights into suspicious activities. By leveraging advanced detection algorithms and real-time monitoring capabilities, our system empowers IT administrators to respond promptly to potential security breaches while mitigating the risk of data compromise and unauthorized access.

In essence, our project represents a proactive step towards enhancing the security posture of organizations in the face of escalating insider threats. By combining innovative technology with strategic deployment strategies, we aim to establish a robust defense mechanism capable of deterring, detecting, and intercepting illegal activities perpetrated by insider employees, thereby safeguarding the integrity and confidentiality of organizational data assets.

I. LITERATURE SURVEY

Some Conclusions we got from the necessary references:

1. Insider Threat Detection Techniques in Cybersecurity

The paper provides a classification of current types of insiders, levels of access, motivations behind it, insider profiling, security properties, and methods they use to attack. It also includes an analysis of major recent studies on detecting insider threats. A thorough analysis of existing literature elucidates the diverse array of insider threat detection techniques employed in contemporary cybersecurity frameworks. From signature-based approaches to anomaly detection algorithms and machine learning models, this research surveys the landscape of insider threat detection methodologies, highlighting their strengths, limitations, and applicability across diverse organizational contexts.

2. Advanced Machine Learning Models for Insider Threat Detection

This article introduces a deep learning-based method for identifying traffic flow at edge nodes. It suggests employing a vehicle recognition algorithm based solely on the YOLOv3 (You Only Look Once) paradigm, extensively tested on a substantial volume of traffic data. The optimization of a DeepSORT (Deeply Simple Open and Real-time Tracking) method is achieved by reutilizing extracted features for multi-item vehicle tracking. To actualize traffic flow identification, a real-time fleet tracking counter is presented, seamlessly integrating vehicles and vehicle tracking methods. On the edge device, the traffic detection achieved an accuracy of 92.0% with an average processing speed of 37.9 frames per second (FPS).

3. Image Analysis for Poultry Disease Detection: A Comprehensive Survey

Introduces a dual-level classification system that excels in real-time classification with high performance. The system comprises level 1 and level 2 classifiers internally. Initially, the level 1 classifier undertakes real-time detection for incoming data flow, yielding moderate accuracy. If the classifier cannot confidently classify the data, the categorization is deferred until the traffic flow ceases. Subsequently, the level two classifier leverages statistical information from the traffic flow for precise classification. The proposed two- level classification system demonstrates superior accuracy and detection speed compared to current approaches.

MATERIAL REQUIREMENTS

Nonfunctional requirements describe how a system must behave and establish constraints of its functionality. This type of requirements is also known as the system’s quality attributes. Attributes such as performance, security, usability, compatibility are not the feature of the system, they are a required characteristic. They are "developing" properties that emerge from the whole arrangement and hence we can't compose a particular line of code to execute them. Any attributes required by the customer are described by the specification. We must include only those requirements that are appropriate for our project. Some Non-Functional Requirements are as follows:

- Reliability

The structure must be reliable and strong in giving the functionalities. The movements must be made unmistakable by the structure when a customer has revealed a couple of enhancements. The progressions made by the Programmer must be Project pioneer and in addition the Test designer.

- Maintainability

The system watching and upkeep should be fundamental and focus in its approach. There should not be an excess of occupations running on diverse machines such that it gets hard to screen whether the employments are running without lapses.

The framework will be utilized by numerous representatives all the while. Since the system will be encouraged on a single web server with a lone database server outside of anyone's ability to see, execution transforms into a significant concern. The structure should not capitulate when various customers would use everything the while. It should allow brisk accessibility to each and every piece of its customers. For instance, if two test specialists are all the while attempting to report the vicinity of a bug, then there ought not to be any irregularity at the same time.

The framework should to be effectively versatile to another framework. This is obliged when the web server, which s facilitating the framework gets adhered because of a few issues, which requires the framework to be taken to another framework.

The framework should be sufficiently adaptable to include new functionalities at a later stage. There should be a run of the mill channel, which can oblige Flexibility is the capacity of a framework to adjust to changing situations and circumstances, and to adapt to changes to business approaches and rules.

An adaptable framework is one that is anything but difficult to reconfigure or adjust because of diverse client and framework prerequisites. The deliberate division of concerns between the trough and motor parts helps adaptability as just a little bit of the framework is influenced when strategies or principles change.

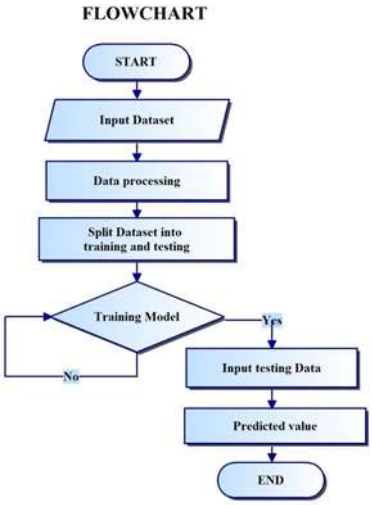


Figure 1. Flow Chart Diagram

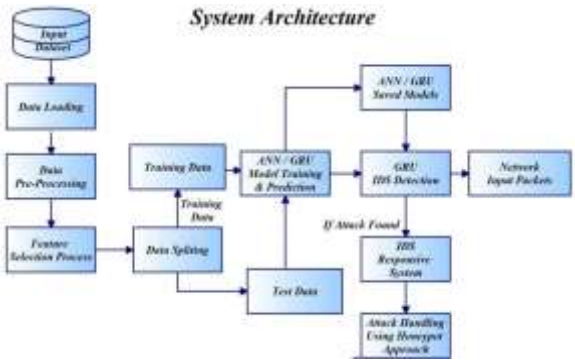
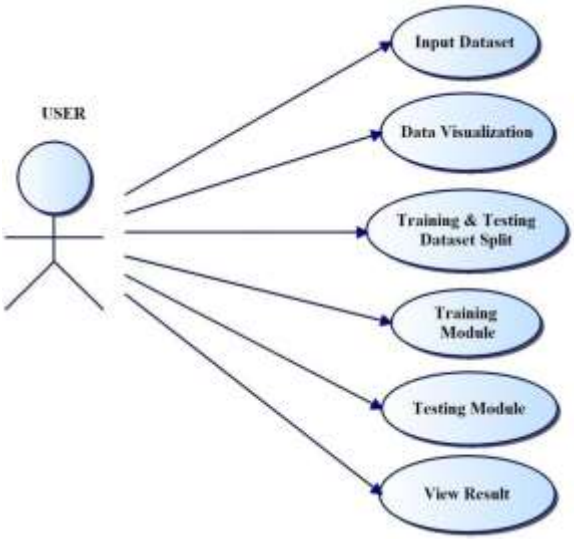


Fig 2 System Architecture

A use case is a set of scenarios that describing an interaction between a source and a destination. A use case diagram displays the relationship among actors and use cases. The two main components of a use case diagram are use cases and actors. shows the use case diagram.

Fig 3 Use Case Diagram User



Data flow diagram

1. A data flow diagram (DFD) is graphic representation of the "flow" of data through an information system. A data flow diagram can also be used for the visualization of data processing (structured design). It is common practice for a designer to draw a context level DFD first which shows the interaction between the system and outside entities. DFD's show the flow of data from external entities into the system, how the data moves from one process to another, as well as its logical storage. There are only four symbols:

2. Squares representing external entities, which are sources and destinations of information entering and leaving the system.

3. Rounded rectangles representing processes, in other methodologies, may be called 'Activities', 'Actions', 'Procedures', 'Subsystems' etc. which take data as input, do processing to it, and output it.

4. Arrows representing the data flows, which can either, be electronic data or physical items. It is impossible for data to flow from data store to data store except via a process, and external entities are not allowed to access data stores directly.

5. The flat three-sided rectangle is representing data stores should both receive information for storing and provide it for further processing.

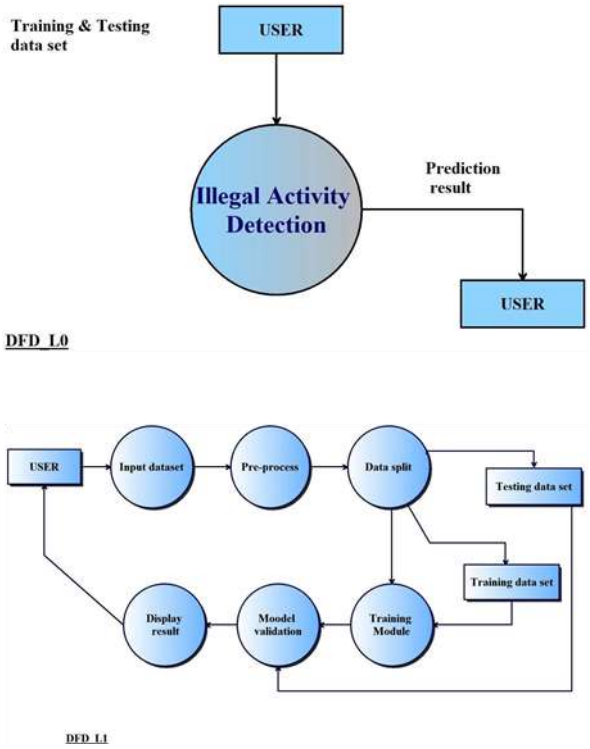
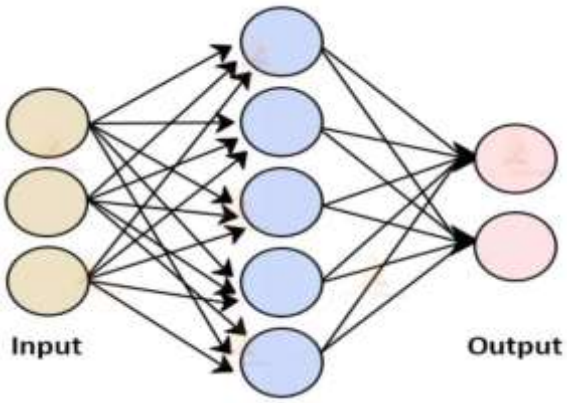


Fig 4 Level 1 Data Flow Diagram

Artificial Neural Networks (ANNs)

Artificial Neural Networks (ANNs) are computational models inspired by the structure and functioning of the human brain. They consist of interconnected nodes or "neurons" organized in layers. The input layer receives data, which is then processed through hidden layers, and finally, an output layer produces the result. Each connection between neurons has an associated weight, which adjusts during training to optimize predictions.

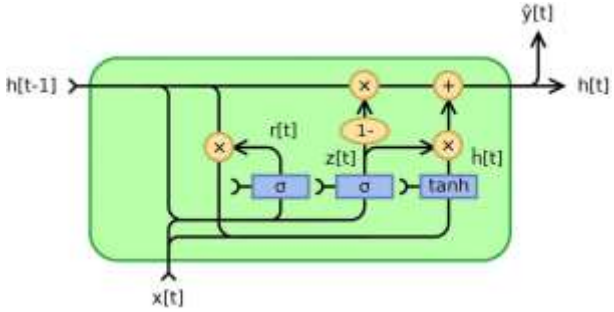


ANNs excel at learning complex patterns in data, making them widely used in tasks like image recognition, natural language processing, and regression analysis. They possess the ability to generalize from training data to make predictions on unseen data. However, ANNs can be computationally intensive

and require substantial data for effective training. Despite their complexity, they are a cornerstone of modern machine learning and have led to significant advancements in various fields.

Gated Recurrent Unit

The above fig 1 shows a GRU represents a specialized architecture within the realm of recurrent neural networks (RNNs), specifically tailored to overcome challenges associated with learning long-term connections between consecutive data sets. Originating from the work of Cho and his colleagues in 2014, GRUs incorporate gating mechanisms, distinguishing them from conventional RNNs. These gating units play a pivotal role in controlling information flow within the network, deciding which information to retain from the preceding time step and which to incorporate anew. Notable for their simplicity in comparison to long short-term memory (LSTM) systems, GRUs combine the hidden state and memory cell into a more compact form.



Renowned for their computational efficiency relative to LSTMs, GRUs efficiently capture sequential dependencies while demanding fewer parameters. This efficiency renders them apt for tasks with constrained computational resources. A salient feature of GRUs is their adeptness in addressing the vanishing gradient problem, crucial for effective learning across extended sequences. GRUs have proven useful in a variety of sequential data applications, including machine translation, sentiment analysis, & speech recognition. They are extensively used in natural language processing jobs. However, the decision between GRUs & LSTMs depends on the demands of the particular task encouraging practitioners to experiment with both architectures to discern their optimal performance for a given application.

CONCLUSION

In conclusion, the development of our approach to detect and intercept illegal activities perpetrated by insider employees represents a critical step forward in enhancing organizational security and mitigating the risks associated with insider threats. By leveraging a dual-server architecture comprising an original server and a honeypot server, we have established a proactive defense mechanism capable of not only detecting and preventing unauthorized access but also tracking malicious activities back to their source. The deployment of dummy files within the honeypot server serves as a strategic deterrent, enticing potential attackers while simultaneously alerting IT administrators to suspicious behavior. Through this innovative approach, organizations can bolster their resilience against insider threats, safeguard critical sensitive data, and uphold the integrity and confidentiality of their information systems. Moving forward, continuous refinement and adaptation of our detection and interception techniques will be paramount to staying ahead of evolving insider threats and ensuring the ongoing security of organizational assets.

FUTURE WORK:

Investigate the efficacy of convolutional neural networks (CNNs), recurrent neural networks (RNNs), and other advanced deep learning architectures for intrusion detection to ascertain their potential benefits compared to ANN and GRU models. ANN and GRU models in real-time network environments and assess their scalability to handle large- scale network traffic while maintaining high detection accuracy. Deep learning-based intrusion detection systems with existing cybersecurity infrastructure, facilitating their adoption and practical implementation in organizations.

ACKNOWLEDGMENT

We would like to thank the University that provided the necessary resources “Dayananda Sagar University” for the opportunities to make the study practical and accessible as desired.

We also thank professor “SHARATH H A” and friends for their collaboration, discussions, and helpful suggestions during a research conference and workshop where preliminary results of this study were presented. Their insights enrich our understanding and inspire us to renew our ways.

REFERENCES

[1] J. Jang-Jaccard and S. Nepal, ``A survey of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973_993, Aug. 2014.

[2] H. E. Kim, H. S. Son, B. G. Kim, J. Cho, S. M. Shin, and H. G. Kang, ``Input-domain software testing for failure probability estimation of safetycritical applications in consideration of past input sequence," IEEE Access,vol. 6, pp. 8440_8451, 2018.

[3] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, ``Deep recurrent neural network for IoT intrusion detection system," Simul.Model.Pract.Theory, vol. 101, May 2019, Art.no. 102031.

[4] H. Hu, H. Zhang, Y. Liu, and Y. Wang, ``Quantitative method for network security situation based on attack prediction," Secur. Commun.Netw, vol. 19, Jul. 2017, Art.no. 3407642.