Insider Attack Detection Using Restricted Boltzmann Machine in Machine Learning

Dayananda Sagar University, dept. of Computer Science and Engineering

Project Proposal Reference No: 46S_BE_2195

Name of project guide:

Prof. Nandini K

Email id: nandini-cse@dsu.edu.in

Name of students with email id:

Adarsha Subrahmanya K K

Email id: adarsh930408@gmail.com

Bharath Kumar N

Email id: bharathkumarbharath075@gmail.com

Bhargav Ram C S

Email id: ramcsbhargav505@gmail.com

Chethan R

Email id: chethanrraj90@gmail.com

Keywords

Restricted Boltzmann Machines (RBMs), Artificial intelligence, Security, Insider Attack, User Interaction Behaviour, Deep Belief Neural Network

Introduction

A malicious insider is a person who has control to sensitive information within an organisation and deliberately utilises it against the interests of the company. This individual could be a partner in company, a contractor, an employee (current or past). On the other hand, a non-malicious insider poses an inadvertent threat as a result of carelessness or neglect in the performance of a typical day-to-day duty. One of the most significant undiscovered dangers to protected data has been found as being this. An insider threat is a former or current employee, contract worker, or business associate who purposefully compromises the integrity, confidentiality or accessibility of the organization's data or information systems and has or had access privileges to the network, system, or data. Insider attacks are destructive behaviours committed by an organisation member with the necessary power.

The security of the intranet has received increasing attention due to the frequency of internal threats. In order to identify intruder who are likely to be able to control the cloud information, the DBN (Deep Belief Neural Network) is used as a classifier. The characteristics of the insider are derived from their behavioural engagement with the programme through the user logs, such as Logon/Logoff activity, File, HTTP (HyperText Transfer Protocol), Email, Device activity. These user logs' aberrant access is computed and utilised as an accent for the categorization of insiders. Using the insider detection approach, it is possible to identify the unreliable or malicious nodes inside the organisation. This method offers protection from harm and detection before an assault.

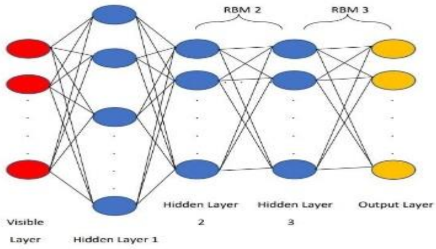
Earlier we had created a user activity and extracted feature from logs and now completed the project by implementing algorithm to DBN and model (DBN) classifies insider and non-insider, if it is an insider our model sends an alert mail to organization.

Objectives

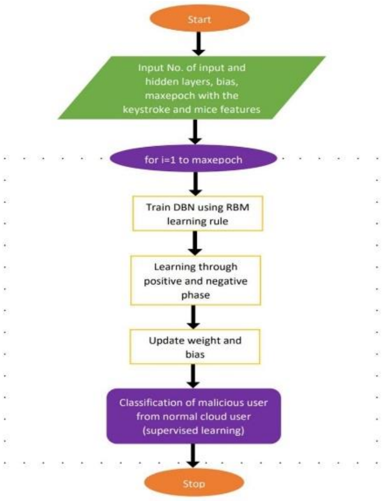
The ML model will be trained and tested using the four effective features date, user, source, action. Detailed study and evaluation of the machine learning technique to detect insider threat will be achieved successfully. The proposed DBN provides better results than other ML algorithms, such as SVM and improved LSTM. This method can complete a user authentication task in a very short time while maintaining high accuracy. High-speed digital processing techniques. Using organization's network, systems, and data negatively to affect the confidentiality of the organization. So, here by introducing the user interaction behavior pattern with a deep belief neural network and detect the malicious behavior and alerts the organization. Model (DBN) classifies insider and non-insider, if it is an insider our model sends an alert mail to organization. Also, our model predicts insider and alerts about them in government sector if insider/current officer from government steal sensitive information and sell it to others.

Methodology

In the cloud network, DBN is utilized to forecast insiders' unauthorized behaviour. DBN are feed forward neural networks with a deep architecture and numerous hidden layers that are machine learning algorithms that mimic deep neural networks but are not the same. Unsupervised, straightforward networks like RBMs (restricted Boltzmann machines). A Deep Belief Network will be created by connecting these restricted Boltzmann machines in a certain sequence. The outcome of the Boltzmann machine's "output" layer is continually fed into the subsequent Boltzmann machine as input. Then, we'll train till it converges and continue using the same strategies until the entire network is built. A network of unpredictable processing units linked in both directions is referred to as a Boltzmann machine, or BM. In this case, a BM's nodes may be classed as visible or concealed nodes. Nodes that are visible signify a part of an observation. For instance, each and every pixel in a computer, each visible node, digital



picture, in an image categorization. However, dependencies among visible nodes that are not modelled by simple pairwise interactions across visible vertices are captured by hidden nodes.

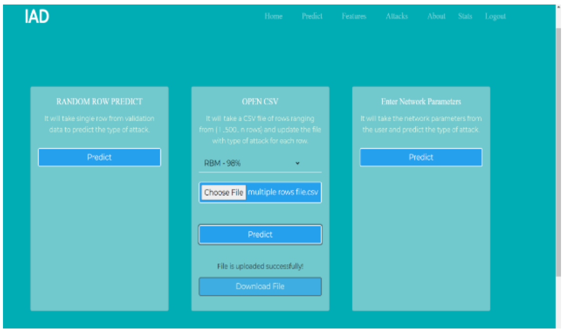

Start
Input No. of input and hidden layers, bias, maxepoch with the keystroke and mice features
for i=1 to maxepoch
Train DBN using RBM learning rule
Learning through positive and negative phase
Update weight and bias
Classification of malicious user from normal cloud user (supervised learning)
Stop

Results and Conclusion

The deep learning model Restricted Boltzmann Machine, Long Short-Term Memory (LSTM), superior version of RNN (Recurrent Neural Network) method are used for binary and multi class classification.

The user enters the hacking parameters in the front end which is designed by using ReactJS. The model predicts the type of attack and gives information about the type of attack to the user. MongoDB is used for storing the data and NodeJS is served as back-end framework.

The project is fully responsive and completely based on session and cookies concepts. Once the user authenticated and logged-in It will not ask the user to enter the login parameters again and again. It asks login parameters only when user click on logout button. And using google oauth 2.0 for user authentication and storing user details in salted hash in the mongoDB.



It will take single row from validation data to predict the type of attack.

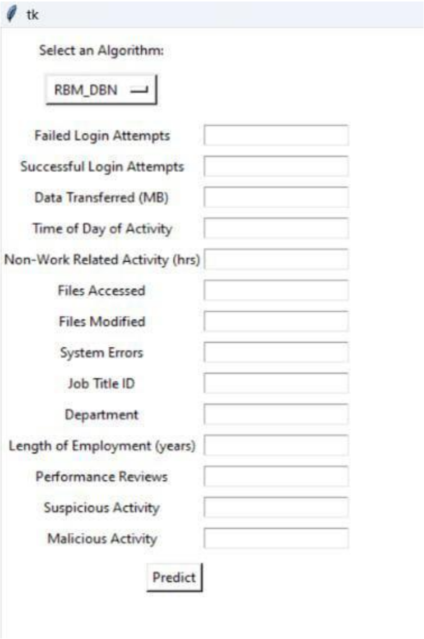
It will take a CSV file of rows ranging from (1..500..n rows) and update the file with type of attack for each row.

RBM - 98%

multiple rows file.csv

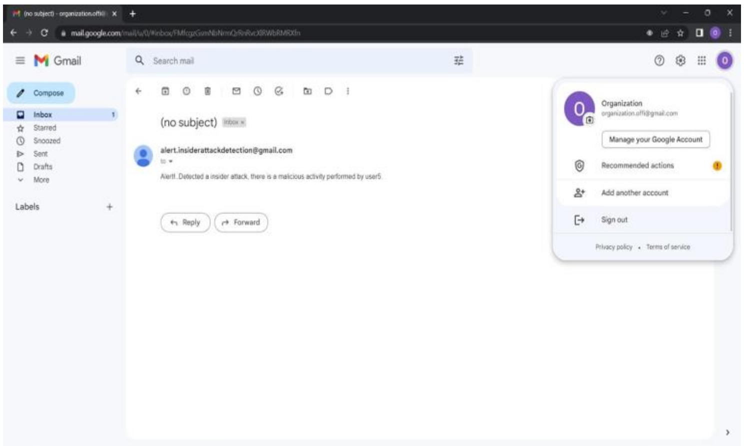
File is uploaded successfully!

It will take the network parameters from the user and predict the type of attack.



Select an Algorithm: RBM_DBN

After filling the values to all fields, model predicts insider and non-insider by popping up 1 and 0 respectively. Eg if it pops up 1, he/she is an insider and our model alerts through mail to the organization. And below is the mail image.



mail.google.com/mail/u/0/#inbox/FMfcgzGwnNbNmrQrRnRvcXRWbRMRXfn

(no subject) Inbox

alert.insiderattackdetection@gmail.com

to

Alert! Detected a insider attack, there is a malicious activity performed by user5

Organization
organization.offi@gmail.com

What is the innovation of the project

This study, likely to do well at detecting insider attacks. Internal attackers frequently exhibit exceptional intelligence by disguising themselves as trustworthy authorities. we assessed an RBM's suitability as a machine learning model. The purpose of this paper was to detect malicious activity using machine learning techniques. We proposed a system pipeline that is capable of identifying malicious users accurately and can adapt to various organizational composition as well as modifications to the structure of the log file. We improved insider threat detection with the use of an automated deep belief neural network.

Scope for future work

This study, likely to do well at detecting insider attacks. Internal attackers frequently exhibit exceptional intelligence by disguising themselves as trustworthy authorities. we assessed an RBM's suitability as a machine learning model. The purpose of this paper was to detect malicious activity using machine learning techniques. We have proposed a system pipeline that is capable of identifying malicious users accurately and can adapt to various organizational composition as well as modifications to the structure of the log file. We improved insider threat detection with the use of an automated deep belief neural network and for future scope we will be implementing feature where organization block all permission of the employee.