JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

VIRTUAL PERSONAL ASSISTANT

1st Angel Barakka J
Assistant professor Department of computer science and business systems, Sri Sairam Engineering College,(Autonomous Institution) ,Chennai, India

2nd Sujan B
Student Department of computer science and business systems. Sri Sairam Engineering College (Autonomous Institution) Chennai, India

3rd Divyesh S
Student Department of computer science and business systems. Sri Sairam Engineering College (Autonomous Institution) , Chennai, India

4th Rohit V R
Student Department of computer science and business systems. Sri Sairam Engineering College (Autonomous Institution) Chennai, India

Abstract-Nowadays there are many software are running in the background of our system in that some of them are vulnerable which are stealing our data so main aim of this virtual personal assistant is to provide an effortless human interaction to control and maintain the system's security from vulnerable software. According to this approach, this a will interact with user by voice input and voice output for denoting any information about the activity, there many type of vulnerable attacks or data stealing methods in that we are mainly focused on software based attacks , wireless networks attacks, tunnel stealing, vulnerable software injunctions . This AI will able to control the system by users input and it will detect the these attacks, we will train a model with data which consist of CPU, GPU, memory , RAM , background data usage , auto boot startups , software size by these data our model will know about the basic usage of every software which are currently running on the system, Apart from this model the we will detecting what type of programs are running in the background, generally it will starts its work from the booting of the system , it will check any programing are acting vulnerably in the background it will detect by trained model also it will detect whether any program is created a tunnel for transferring details these tunnel communication detections are done by continuous analysis of secure shell activity and also by detecting that any signals are data transfers are occurred by any program continuously and apart from wireless attacks it will detect the unknown user activities make a required action to secure the data for making these secure action this AI will send a notification to owners mobile which is having APK which will help to make required action through that APK the user can do some necessary action like taking a picture of the attacker, also control their laptop through mobile.

Keyword: Virtual Personal Assistant, Vulnerable detection, tunnel stealing, wireless network data steal connection

I. INRODUCTION

1.1Objective

In current world, most of the peoples are maintaining their data in their devices like laptops and computers because they having too many software and program they can't find vulnerable program among these. The purpose of this study is to make a virtual assistant which will help the user to make effortless interaction with the system to control and maintain the system security through this assistant they can easily detect the vulnerable activity of any program that are exist in the system . It will detect it by a calculating it usage, performance and check with a trained model also it will interact with the use through voice input and output.

1.2Motivation

Nowadays, peoples use many software and programs, in that many of them are running in the background of the system. Some of these background services are stealing the user's data and sent that data through a wireless network communication or through tunnels. Most these programs are injected by social hacking or social engineering so most of the users doesn't know about these programs are running in their system.

1.3Relevance of the project

Network Traffic Analysis (NTA) tools use machine learning to analyze network traffic and identify suspicious activity that may indicate a cyber attack. It only detect the tunnels

Some virtual assistants, such as Amazon's Alexa for Business and Microsoft's Cortana, can integrate with security tools to monitor network activity and detect potential security threats. For example, Alexa for Business can integrate with AWS security services to provide security alerts and enable security automation.

Other virtual assistants, such as Cisco's Spark Assistant, are designed specifically for security purposes. Spark Assistant uses machine learning algorithms to monitor network traffic and detect suspicious activity, such as unauthorized access attempts and data exfiltration.

1.4 Design Methodology

For detecting the vulnerable activity we are using neural network to train a model , in this neural network model it will calculated the output by matrix calculation with weight sum of the inputs those inputs are usage and performance of the program in the background and it will apply to a activation function includes sigmoid which help to find value of multiple layers in the network and it will apply Gaussian distribution for find a probable value of the input, this model will also involves in the back propagation. With this model we will find the vulnerable software or program through the following flow

A. Booting: In the booting of the system it will starts and at first it will detect all the current running programs and analyze the usage and performance of the program in the background by the trained model and stop the some of the unwanted process in the booting process

B. User interaction: This assistant will have full user interaction through voice input and output, this interaction will help the user to know about which program is suspected for vulnerable activity and what can be do with that to solve. User can access system through their voice

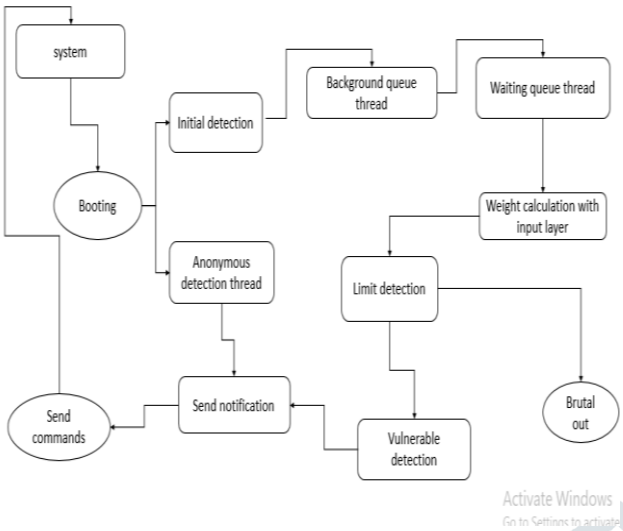
C. Limit detection: In this, the assistant is doesn't always check the system performance. It will have a queue and in that queue it will add instance of a program when it running on the background , it will have a limit for a system utilization if any of the program in that queue have exceed the limit means it will check the vulnerability and if it doesn't vulnerable means it will remove from the background and added to the waiting and the waiting queue is dynamically typed in that waiting queue every instance will be limited with a different or same parent process and then it will check whether this waiting queue is cross their parent limit if it cross means it will indicate to the user that it is vulnerable suppose in the waiting queue any of the instance have reached the normal limit of their parent means it will remove from the waiting queue and add to the background queue also if any of the process is closed means its instance form the background queue will be removed

D. New entrance: If any software is installed or starts working in background means it will be verified fully for the first time and then it will attend to the background queue by their instance, these regular performance are stored in the local storage for further weight calculations, by storing these details won't take too much space because these are text content and it will only data of past 3 months

E.Tunnel detection: Tunnel ways data stealing is one of silent way of data stealing because it doesn't affect any performance or usage of the system because in this method they will create a network tunnel from their system to the user's system through this tunnel they can easily steal data. But our assistant will monitor the network layer of the system to detect any unwanted response is passing through the use the tunnels, by analyzing the network activity we can find the unwanted tunnels. Also it will find the tunnels by which port is consuming resource like TCP and which port is often bypass the firewall.

F. Remote Notification: This assistant will send notification to the users mobile through a mobile application connected with this assistant, it will send notification only if it detects any anonymous user background queue is not empty when it is sign off also the user can set option that he can remotely access the system when someone try to unlock his system. From that mobile application the user can make their laptop shutdown, end all process, sign off, restart and also the can take the report of the system performance, take screen short, take a picture of who using the system.

G. Brutal out: Some of the programs are cause some performance damage in the system, assistant will also detect it by the instance of the program in the background process queue if this instance exceeds the limit and return from more value from the model out means the assistant will not this program is a dangerous programs and brutally stop this program and add to a warning array and when a new program enter in the background queue means assistant will check whether it's instance exist in the warning array, this array is not general for all users it separate for every different user and this array is stored in their storage



This assistant will also use a local storage and global storage in the local storage all the queue, array are stored using sqlite database for better analyzing of the output value of the network model. And the global storage is use for further improvement in the network model so that the appropriate value will accurate these global storage are consist of the value that use in calculation of the weights in the network. It doesn't take more space in the local device because the assistant will have the data of past 3months only also most of them are text data, also this assistant will always run in the background of the system and it doesn't take too much CPU and RAM because it will use model when the limit exceed for an instance of program also other than that it will work with some detection process for that it won't take too much of CPU and RAM

These are the process which will help to handle the software vulnerability, apart from this, our assistant can detect the unknown user activity by storing, this method is not always call it will call only when any file transferring occurs.

1.5 Abridgement:

An effortless interaction with system to control and secure the system. Based on the background process queue which consist of a instance these process and it will analyze the limit of these instance and when a process exceed its limit will calculate the vulnerability level by the neural network model by adding the weights sum input of the different layers of the network and then it will return the value based on the Gaussian distribution. By this value we can identify that this instance of a program is vulnerable are not also this system is not always running the model to verify the instance safe or not it will add this instance to a queue and then it will dynamically allocate the limit and also it will do some brutal out for some danger programs which are running the background in the system. It will monitor the network layer of the system to detect any unwanted response is passing through the use the tunnels, by analyzing the network activity we can find the unwanted tunnels. Also it will find the tunnels by which port is consuming resource like TCP and which port is often bypass the firewall. This assistant will send notification to the users mobile through a mobile application connected with this assistant, it will send notification only if it detects any anonymous user background queue is not empty when it is sign off also the user can set option that he can remotely access the system when someone try to unlock his system.

II.Related Works

User and Entity Behavior Analytics (UEBA): UEBA tools use machine learning algorithms to analyze user behavior and identify anomalies that may indicate a security threat. Network Traffic Analysis (NTA): NTA tools use machine learning to analyze network traffic and identify suspicious activity that may indicate a cyber attack.Security Information and Event Management (SIEM): SIEM tools collect and analyze data from various sources to identify potential security threats. Endpoint Detection and Response (EDR): EDR tools use machine learning to monitor endpoints such as laptops, desktops, and servers for suspicious activity that may indicate a security threat. Threat Intelligence Platforms: These platforms use machine learning algorithms to analyze data from various sources and provide insights into potential security threats.

These are the mainly focused on the vulnerability detection and some of the systems are provide an AI assistant and also the vulnerability detection such as Amazon's Alexa for Business and Microsoft's Cortana, can integrate with security tools to monitor network activity and detect potential security threats. For example, Alexa for Business can integrate with AWS security services to provide security alerts and enable security automation. Other virtual assistants, such as Cisco's Spark Assistant, are designed specifically for security purposes. Spark Assistant uses machine learning algorithms to monitor network traffic and detect suspicious activity, such as unauthorized access attempts and data exfiltration. Virtual assistants can also be used to educate and train employees on cyber security best practices. For example, a virtual assistant can provide automated security awareness training to employees, such as tips on how to identify and avoid phishing emails or how to use strong passwords. But these are not focused on the social engineer tool data stealing and secure tunnel transferring.

III. Existing and Proposed System

3.1. Existing System

In the ranking of virtual assistant , Google assistant , alexa are top for both of them are very well in finding vulnerable activities but it they find the vulnerable activity by the harmful data transferring and it will most like prevent the user from installing those software or program in their system, also they will analyzer the a program or software before installing it but these detection are very good only in the case harmful injection, in recent days most of attack are not happening in the harmful way they were using social engineering and enter into our system friendly and get the data through wireless network communication and through tunnels, for particular case tunnel way data transfer detection there are some existing system are available and they are User and Entity Behavior Analytics (UEBA),Network Traffic Analysis (NTA),Security Information and Event Management (SIEM),Endpoint Detection and Response (EDR),Threat Intelligence Platforms. These software are not handling the wireless network communication data stealing and some the security system are not providing the user interaction where user doesn't know about how these software are entered into their systems.

- It doesn't detect the wireless data sharing programs
- It only if the program have make an any harmful action

3.2. Proposed System

A virtual assistant which will detect the data stealing and detect the vulnerable and provide effortless human interaction through voice input and output. For detecting the vulnerable activity we are using neural network to train a model , in this neural network model it will calculated the output by matrix calculation with weight sum of the inputs those inputs are usage and performance of the program in the background and it will apply to a activation function includes sigmoid which help to find value of multiple layers in the network and it will apply Gaussian distribution for find a probable value of the input, this model will also involves in the back propagation. This is an optimization algorithm used to adjust the weights of the network based on the error between the predicted output and the actual output by the performance input. We calculate the gradient of the cost function with respect to the weights, and adjust the weights in the direction of the steepest descent. the assistant is doesn't always check the system performance. It will have a queue and in that queue it will add instance of a program when it running on the background , it will have a limit for a system utilization if any of the program in that queue have exceed the limit means it will check the vulnerability and if it doesn't vulnerable means it will remove from the background and added to the waiting and the waiting queue is dynamically typed in that waiting queue every instance will be limited with a different or same parent process and then it will check whether this waiting queue is cross their parent limit if it cross means it will indicate to the user that it is vulnerable suppose in the waiting queue any of the instance have reached the normal limit of their parent means it will remove from the waiting queue and add to the background queue also if any of the process is closed means its instance form the background queue will be removed

a. Sockets:

By using these sockets this assistant find which port are busy and which port are connected with a tunnel, sockets help to handle the port so the tunnels are connected with a port to transfer the data from the user's system to their server

b. Neural Network:

To detect the vulnerable activity , we are using the background program's instance performance and usage details with this value as the input of the network layer we will find the weight matrix for the value. This model is not always called and it will call only the limit exceed by particular instance in the queue.

c. TTx3:

This will help to handle the voice output and user interaction to handle this assistant also it uses the voice recognition to take the user's voice input and understand and convert it into a command

IV. Result

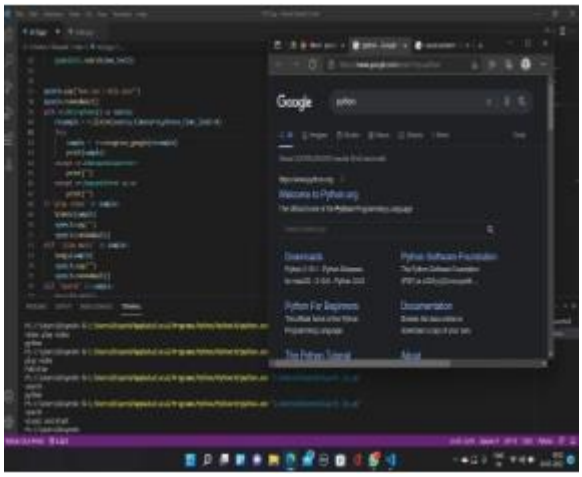
In the booting of the system it will starts and first it will detect all the current running programs and analyze the usage and performance of the program in the background by the trained model and stop the some of the unwanted process in the booting process

Tunnel ways data stealing is one of silent way of data stealing because it doesn't affect any performance or usage of the system because in this method they will create a network tunnel from their system to the user's system through this tunnel they can easily steal data. But our assistant will monitor the network layer of the system to detect any unwanted response is passing through the use the tunnels, by analyzing the network activity we can find the unwanted tunnels. Also it will find the tunnels by which port is consuming resource like TCP and which port is often bypass the firewall.

User can remotely access the system when someone try to unlock his system. From that mobile application the user can make their laptop shutdown, end all process, sign off, restart and also the can take the report of the system performance, take screen short, take a picture of who using the system.

This assistant will also use a local storage and global storage in the local storage all the queue, array are stored using sqlite database for better analyzing of the output value of the network model. And the global storage is use for further improvement in the network model so that the appropriate value will accurate these global storage are consist of the value that use in calculation of the weights in the network. It doesn't take more space in the local device because the assistant will have the data of past 3months only also most of them are text data, also this assistant will always run in the background of the system and it doesn't take too much CPU and RAM because it will use model when the limit exceed for an instance of program also other than that it will work with some detection process for that it won't take too much of CPU and RAM

These are the process which will help to handle the software vulnerability, apart from this, our assistant can detect the unknown user activity by storing, this method is not always call it will call only when any file transferring occurs.



This assistant will send notification to the users mobile through a mobile application connected with this assistant, it

will send notification only if it detects any anonymous user background queue is not empty when it is sign off also the user can set option that he can remotely access the system when someone try to unlock his system. From that mobile application the user can make their laptop shutdown, end all process, sign off, restart and also the can take the report of the system performance, take screen short, take a picture of who using the system.

V. Future Enhancement

This algorithm will done by taking the current usage value and detect the whether it is vulnerable or not by neural network model but in the future enhancement we will make an virtual assistant which will fully monitor the system analysis whether anything is goes wrong and correct it like a system doctor.

VI. Reference

[1] " Virtual Personal Assistant Design Effects on Memory Encoding" A.F. Chesser,,K.N. Bramlett;,A. Atchley;,C.E. Gray;N.L. Tenhundfeld

2022 Systems and Information Engineering Design Symposium (SIEDS)

[2]" Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home)" Veton Këpuska,Gamal Bohouta-2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).

[3]" VOICE ASSISTANT USING PYTHON" Aabhas Kumar;,Damandep Kaur;,Abhishek Kumar Pathak, -2022 International Conference on Cyber Resilience (ICCR).

[4]" Design and Development of Intelligent Voice Personal Assistant using Python" Vadaboyina Appalaraju,V Rajesh,K Saikumar,P. Sabitha,K Ravi Kiran- 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N).

[5]" Virtual Voice Assistant In Python (Friday)"Shailaja Uke,Hrishikesh Lokhande;Durva Lohar;Devansh Lathiya;Aditya Langhe;Tanmay Lautawar;Pranali Likhitkar-2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA).

[6]" Virtual assistants and privacy: An anticipatory ethical analysis"Richard Wilson;Ion Iftimie-2021 IEEE International Symposium on Technology and Society (ISTAS).

[7]" Desktop based Smart Voice Assistant using Python Language Integrated with Arduino" Akash S;Neeraj Jayaram;Jesudoss A-2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS).

[8]" An IoT based Smart Home with Virtual Assistant"T.M.N. Vamsi;B. Suchitra;Sai Kumar;K.V.V. Varma;K.N.S.Harshit Kumar-2021 6th International Conference for Convergence in Technology (I2CT).

[9]" Intelligent Voice Assistant by Using OpenCV Approach",CH.M.H. Saibaba;Saiyed Faiayaz Waris;S.Hrushikesava Raju;VSRK Sarma;Vijaya Chandra Jadala;Chitturi Prasad-2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC).

[10] Arindam Roy, Dharmpal Singh, Sudipta Sahana."Educational Assistance Bot", Journal of Physics:Conference Series, 2021.

[11] Tom M. Mitchell 2017,"Machine Learning",McGraw Hill pp 1992.

[12] Yusuf Ugurlu, Murat Karabulut, Islam Mayda"A Smart Virtual Assistant Answering Questions About COVID-19" Mathangi Sri "NLP In Virtual Assistants".