Engineering and Scientific International Journal (ESIJ)
Volume 10, Issue 4, October – December 2023
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Efficient Model for Intrusion Detection and Prevention in Wireless Network

N. Prabha[#1], M.Sharmila[*2], M. Arulprabhu[*3]
[1,2]*Students,* [3]*Faculty*
[1,2,3]*Department Of Computer Application*
K.S.R College Of Arts and Science For Women Tiruchengode, Tamil Nadu

Abstract — Intrusion detection is a security management system for a computer or computer networks. An Intrusion Detection System (IDS) is a key to detect and prevent malicious activities. The network must be trained to detect intrusions. Intrusion Prevention System (IPS) is defense mechanisms to detect malicious packets within network traffic and stop intrusions, blocking the aberrant traffic automatically before it does any. Network Intrusion Detection System (NIDS) used as a tool that provides the intrusion detection functionality by sniffing the network traffic in real-time and it performs intrusion detection through network connections and outside the host machine is more resistant to attacks by malware. In a traditional network, attacker's entry monitoring, Intrusion detects and alert to the administrative user for network malicious activity by deploying IDS on key network points on user site. Cloud network IDS has to be placed at server site and entirely administered and managed by the service provider. Proposed efficient IDS administered and monitored by the user and expert advice for wireless sensor network administrator.

Keywords: *IDPS; HIDS; NIDS; Behaviour Profile; Saas; Paas; Iaas.*

1. Introduction

Highly resilient and scalable environments to be used by enterprises in a massive amount of ways which provides the distributed internet based platforms defined by Shiva rama krishna et.al for "clouds". Shristi Shrivastav and Gagan Dhawan defined the term "Cloud computing" is a vast area, use the resources with cost-effectively. The resources can be shared anywhere at any time by the service provider. The IT world with its services that provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability has revolutionized by "cloud computing" which is defined by Parag et.al. Vaibhav Kant Singh and Devendra Kumar Singh defined "Cloud computing" is a collection of various technologies like remote access, network virtualization etc additionally includes group of cluster and grid which have many computers or server forming an infrastructure. Ayman Ali, Saif Eldin Fattoh Osman states the national institute of science and technology (NIST) had defined cloud computing as "A model for enabling ubiquitous, on demand network additionally convenient access to a communal pool of configurable resources that has been quickly provisioned and released with minimal effort".

Cloud computing is incessantly developing and there are numerous major cloud computing suppliers who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service and Infrastructure-as-a-Service (IaaS). The table 1 illustrates the cloud computing service and the service providers.

The dietary patterns of the world population have been on transition due to the high consumption of ready-to-eat foods, which have increased levels of fat and sugar, and lower intake of unprocessed foods, such as fruits, vegetables, tubers, and cereals (Monteiro *et al*., 2011). The potential cause of the pandemic of overweight, obesity and rapid rise of related chronic diseases especially in under developed countries is the corresponding increase in the production, processing and consumption of readily available 'fast' or 'convenience' ready-to-eat or ready-to-heat processed food and beverage products (WHO, 2010). Ultra-processed foods are defined within the NOVA classification system, which groups foods according to the extent and purpose of industrial processing. NOVA is a food classification system developed by researchers at the university of Sao Paulo Brazil (Monteiro *et al.*, 2011).

Table 1: Cloud Computing Service

Service Model	Describe	Provider
SaaS	A Service that provides Software	Google Apps, IBM, Microsoft 365
PaaS	A service in the form of a platform that users can use to create applications	Amazon Web Service, Google Apps
IaaS	A service that offers a physical box server and virtual computer	VMware, CSC, Bluelock

DOI: **10.30726/esij/v10.i4.2023.104001**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

A practical way to identify an ultra-processed product is to check to see if its list of ingredients contains at least one item characteristic of the NOVA ultra-processed food group, which is to say, either food substances never or rarely used in kitchens (Monteiro *et al.*, 2015). Ultra-processed fast foods and soft drinks are the main business of transnational and big national catering chains, whose outlets are also often open until late at night, and whose products are designed to be consumed also in the street, while working or driving, or watching television (Allemandi, 2018).

The consumption of ultra-processed foods are increasing rapidly, replacing use of traditional or indigenous, culturally acceptable freshly cooked food (Moodie *et al.*, 2013). These Ultra-processed products are characteristically formulated from 'refined' and 'purified' ingredients freed from the fibrous watery matrix of their original raw materials.

They are formulated to be sensually appealing, hyper-palatable, and habit-forming, by the use of sophisticated mixtures of cosmetic and other additives, and state of the craft packaging and marketing (Baker and Friel, 2016).

The World Health Organization stated that sugary drinks, energy dense snacks and 'fast food', all of which are ultra-processed, are key drivers of obesity, diabetes, cardiovascular diseases and certain cancers (WHO, 2018). Most people crave and consume more of these ready to eat or convenient foods not necessarily because they want them but because they see these ultra-processed foods are the fastest and easiest food to prepare or consume. Others also consume them just to save time while others take them as meal to meet up their daily dietary requirement. There is a major concern on the increase in the prevalence of non-communicable diseases like hypertension, diabetes and stroke amongst adults, hence this study assessed the consumption of ultra-processed foods, dietary pattern and anthropometric status of adults aged (20-49 years) in Ikwuano Local Government Area, Abia State.

2. Literature Survey

Parag et.al proposed a new multi-threaded distributed cloud IDS model to handle large scale network access traffic, administrative control of data and application in cloud which analyzed the data packets and makes the reports efficiently by integrating behavior analysis to detect intrusions.

Amjad Hussain Bhat et.al proposed an IDS using Machine Learning Approach (MLA) for virtual machines on cloud computing and it is feature selection over events from Virtual Machine Monitor (VMM) to detect anomaly in parallel to training the system so it learn new threats and update the model. The model carried out on NSL-KDD'99 datasets using Naive Bayes Tree (NB Tree) Classifier and Hybrid Approach (HA) of NB Tree and Random Forest.

Michal Korcak et.al deals the security issues of small office and home office wireless networks. The objective is to design and evaluate wireless IDPS with the help of packet injection method. While using proposed IDPS system 95% decreased the attacker's traffic.

Shiva rama krishna et.al presented in their paper the problem and challenges in IPS and they were researched the issues like heterogeneous sensor, distributed sensor, and combine hybrid early detection/ prevention mechanism with other approaches. They focused on their future work as accuracy and precision with the algorithms based on behavior-based prevention and the data set of real-traffic network.

Trupti Dange and Pankaj Bhalerao proposed multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based systematic models and reconfigurable virtual network-based countermeasures. *Amna Riaz et.al* fixed the aim for their paper is to review IDS techniques which have been used in the cloud. To achieve this objective two different steps followed. At beginning defined the limitations and unique characteristics of the techniques, and then established the criteria to evaluate IDS architectures. Finally the issues and drawbacks comprehended from the evaluation in cloud environment were discussed.

Mohamed Faisal Elrawy et.al proposed the new technique which is able to help by the protection of the distributed virtualization network infrastructures and evaluates the techniques like various ways to detect the potential attack activities and provides an efficient solution how to link the anomality detectors and hypervisors. The model provides the way to eliminate the problems without having to shutdown the running on virtual machines. The greatest benefit of such solution stands in the runtime protection without suppressing more services, than it's necessary. *Shivam Singh et.al* illustrates the novel Intrusion Detection (ID) method i.e., Calibration Factors-based Intrusion Detection (CFID) for cloud networks. The research portrayed the significant scope of the model CFID to detect the intrusion activities listed as remote-to-Local, Virtual-Machine-Trapping and Port Scanning.

3. Related Work

Parag et.al states Cloud computing has three basic abstraction layers i.e. system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications) and Cloud computing

DOI: **10.30726/esij/v10.i4.2023.104001**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

have three service models i.e, Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS providing platform to the users on which applications can be developed and run. IaaS have maintaining large infrastructures and deliver services like hosting servers, managing networks and other resources to clients. SaaS model makes agonize free of installing and running software services on its own machines.

3.1 Types of Attacks

3.1.1 Denial-of-Service (DOS) Attacks

DOS attacks tries to deny the authorized users from promoting the requested service and the advanced Distributed Denial of Service occurs in a distributed environment that the attacker floods or sends the server with numerous connections that request to knock the target system. The types of Denial of Service (DOS) attacks are as follows

3.1.1.1 SYN Attack

SYN attack is also defined as Synchronization attack in that, the attacker sends the flood of SYN request to the destination to use the resources of the server and to make the system unresponsive.

3.1.1.2 Ping of Death

The intruder sends a ping request which is larger than 65,536 bytes to the targeted system which causes the system to crash. 56 bytes or 84 bytes as formal size in case of considering Internet protocol header.

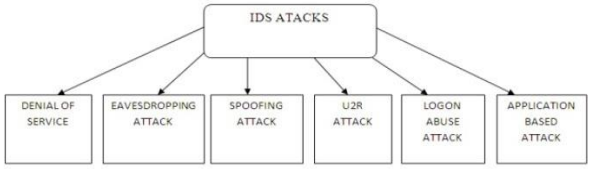

Fig 1: Types of Attacks

3.1.2 Eavesdropping Attacks

Eavesdropping attacks by the attacker which is the scheme of interference in communication and the attacks done in telephone lines or through email.

3.1.3 Spoofing Attacks

In spoofing attacks, the attacker depicts as an additional user to falsify the data and take advantages on illegal events in the network. An example, IP spoofing is the system communicates with a trusted user and provides access to the attacker.

3.1.4 User to Root Attack (U2R) or Intrusion attacks

In User to Root attack, an intruder tries to access the system or route through the network. When a web service receives more data than it has been programmed to handle which leads to loss of data which is occurs in buffer overflow attack.

3.1.5 Logon Abuse Attacks

A logon abuse attack neglects the authentication and access control mechanisms and grant more advantages to the user.

3.1.6 Application-Level Attacks

In application-level attacks, the attacker targets the application layer disabilities.

4. Proposed Model

The traditional cloud IDSs is not efficient to handle the large data flow. The most known Intrusion Detection Systems (IDS) were single threaded. Due to rich dataset flow and there is a need of multi-threaded IDS for Cloud. IDS for Cloud placed in Cloud server and exclusively administered and managed by the service provider. In this scenario, the attacker manages and damage user's data, the cloud user not be notified directly. The intrusion data communicated through the service provider and user has to rely. The cloud service provider may not like to inform to the user about the loss. The third party monitoring service tools were used to monitoring and alerting to cloud user and service provider.

Proposed multi-threaded cloud IDS which is administered and monitored by ID monitoring service and it provides alert reports to cloud user and cloud service provider. In order to resolve the issues, an efficient and reliable distributed Cloud IDS model is proposed and which is the combination of Grid and Cloud computing concepts. The data request has been provided by the service provider in time. The major part of the research work is providing the security for Cloud using Grid Technology. The Security have to achieved by two phase, namely Behavioral and Knowledge.

Behavior Analysis: Using this method, recognize expected legitimate use or a severe behavior deviation. The network must be correctly trained to detect intrusions efficiently using sample data set to identify the intrusions by the learner. However, focus on identifying user behavioral patterns and deviations from such patterns which covers a wider range of unknown attacks.

DOI: **10.30726/esij/v10.i4.2023.104001**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Knowledge Analysis: Using an expert system describe a malicious behavior with a rule. The advantage of this intrusion detection is that, can add new rules without modifying existing ones. Intrusion Detection (ID) is a tool for security management system of computers and networks. IDS are collecting and analyzing the information from various locations of computer or a network to identify possible security violation which includes both intrusions from outside the organization and misuse from inside the organization. ID uses vulnerability assessment i.e., sometimes referred to as scanning, which is a technology for assess the security of a computer system or network. Intrusion detection functions as follows,

- Analyzing system configurations and vulnerabilities
- Monitoring and analyzing system and user activities
- Assessing system and file integrity

Through the above survey decided to identify the intrusion and improve the accuracy and efficiency of existing model behaviour profiling algorithm technique have been implemented. Using behaviour profiling algorithm the network administrator have been collect the composite data of the network users behaviour which is in the form of log files.

4.1 Proposed Behaviour Profiling Algorithm

Step 1: Logs entropy (or Information gain) from Server
Step 2: Identify the Process and respective PID (Process Identification Number)
Step 3: Identify the IP (Internet Protocol) Address for each Process using PID.
Step 4: Identify the TCP/ UDP transformation Process
Step 5: Identify the Active Time and Response time for each process.
Step 6: Identify the Data Packet transformation and Data Packet Loss
Step 7: Trace the IP Address and its behaviour of Transformation
Step 8: Classify the Authorised and Unauthorised Transformation
Step 9: Make the Prevention from the Unauthorised Transformation

To implement the proposed algorithm as an expression the following acronyms have been used. The Nodes in the Wireless Network is marked as NWLNet, the quantity of Servers in the Wireless Network is noted as NSWLNet, the quantity of Nodes connected in the Server is represented as NNS, the quantity of Normal Nodes in the Wi-Fi Network is denoted as NNNWLNet, the Number of Process running in Nodes is marked as NRPN, the quantity of Process using TCP is mentioned as NPRTCP, the quantity of Process using UDP is represented as NPRUDP, the quantity of Data Packets Transferred is marked as NDPTrans, the quantity of Data Packets Loosed is represented as NDPloss, the Authorised Transformation is marked as ATrans and Unauthorsed Transformation is denoted as UTrans. By identifying the servers count (NSWLNet) that are connected in the wireless network and the number of client nodes (NNNWLNet) connected in the network which lead to identify the nodes (NWLNet) are connected in the wireless network.

$$\sum NWLNet = \sum NSWLNet + \sum NNNWLNet \quad (1)$$

By identifying the number of process running along with TCP (Transmission Control Protocol) (NPRTCP) and the number of process running along with UDP (User Datagram Protocol) (NPRUDP) which leads to identify the Number of process running in the client nodes (NRPN) which are connected in the server.

$$\sum NRPN = \sum NPRTCP + \sum NPRUDP \quad (2)$$

The number of process running along with TCP (Transmission Control Protocol) (NPRTCP) can be identified by the difference between the Number of process running in the client nodes (NRPN) which are connected in the server and the number of process running along with UDP (User Datagram Protocol) (NPRUDP)

$$\sum NPRTCP = \sum NRPN - \sum NPRUDP \quad (3)$$

The number of process running along with UDP (User Datagram Protocol) (NPRUDP) can be identified by the difference between the Number of process running in the client nodes (NRPN) which are connected in the server and the number of process running along with TCP (Transmission Control Protocol) (NPRTCP)

$$\sum NPRUDP = \sum NRPN - \sum NPRTCP \quad (4)$$

To get the quantity of authorized transactions which is running in a personal computer or intranet server along with TCP, first identify the number of processes are running along with TCP (NPRTCP), next identify the total number of process running in the nodes (NRPN). The Sum of difference between NPRTCP and NRPN will be found by using the IP (Internet Protocol). To get the quantity of authorized transaction processes which is running in a web server along with TCP, first identify the total number of processes are running along with TCP (∑NPRTCP), next identify the total number of process running in each nodes (∑NRPN). The difference between ∑NPRTCP and ∑NRPN identified using IP of nodes.

$$\sum ATrans = IP \in NPRTCP \sim \sum NRPN$$

(or)

$$IP \in \sum NPRTCP \sim \sum NRPN \quad (5)$$

DOI: **10.30726/esij/v10.i4.2023.104001**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

To identify the quantity of authorized transaction processes running in a personal computer or intranet server along with UDP, first identify the number of processes are running along with UDP (NPRUDP), next identify the total number of process running in the nodes (NRPN). The difference between NPRUDP and NRPN has been found by using IP of nodes. To identify the quantity of authorized transaction processes running in a web server along with UDP, first identify the total number of processes are running along with UDP (∑NPRUDP), next identify the total number of process running in each nodes (∑NRPN). The sums of difference between ∑NPRUDP and ∑NRPN identified using each node IP.

$$\sum ATrans = IP\epsilon\ NPRUDP \sim \sum NRPN$$

(or)

$$IP\epsilon \sum NPRUDP \sim \sum NRPN \quad (6)$$

To identify the number of unauthorized transaction (∑UTrans) processes running in a personal computer or intranet or web or internet server, first identify which IP (Internet Protocol) is entering and processing its process in each nodes in the network except the Administrator IP. Next analyse the IP's behaviour like the IP downloads and uploads its file to the nodes, it makes the data transaction losses, it generates the deadlock conditions in the network, it traces the system supporting files. If an IP performs one of these activities in the network, the administrator simply locks this IP activity because the IP address is attacker/intruder.

$$\sum Utrans = IP \sim NNS$$
$$= IP \sim NWLNet$$
$$= IP \sim NSWLNet$$
$$= IP \sim NNNWLNet \quad (7)$$

To find the performance and efficiency of the existing and proposed model (ExE) identified by using the model weak data and Synthetic data and find the Percentage of the existing model (PExE) by using (ExE)

$$ExE = \frac{\varepsilon\ Weak\ Data}{\varepsilon\ Synthetic\ Data} * 100 \quad (8)$$

$$PExE = 100 - ExE$$

5. Result and Discussion

Using the proposed model the cloud network users and their activities has been traced. The data packets transformation status from user to server and server to user i.e., received and sent details has been analyzed. Figure 5 illustrates the information about the transformation of packet in the cloud network. Through that the administrators have identified the authorized and anomaly users with the help of log files. If the log files has the error information in the entry point of the file system which has the server. The information has been stored into the database and which is called as Behaviour profile of the user. At the same time the network users activities has been analyzed. If in the network numerous users have been accessed a file, the server moves to the "In Traffic". Otherwise the server moves to the "Out Traffic".

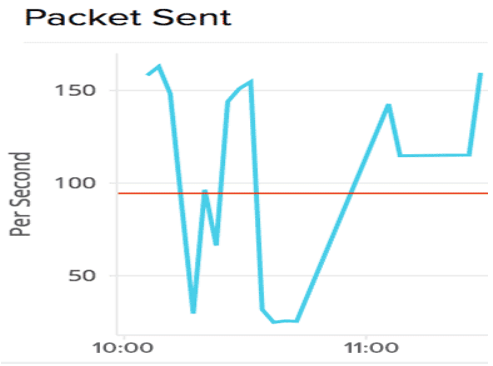

Fig 5: Transformation of packet in the cloud network

The following figure 6 illustrates the information about the transformation of data (in bytes) in the cloud network during In Traffic and Out Traffic.

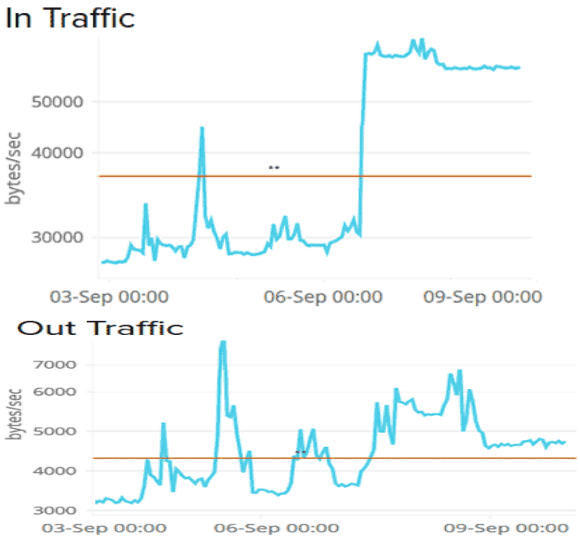

Fig 6: Transformation of data (in bytes) in the cloud network during In Traffic and Out Traffic

The following Figure 6 illustrates the information about the average transformation of packet in the cloud network.

DOI: **10.30726/esij/v10.i4.2023.104001**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

6. Conclusion

The conclusion of this article is that, the efficient algorithm to detect the intrusion is behaviour profiling algorithm, the algorithm while join with the statistical approach model, it produces above 90% of the efficiency in the wired network, above 96% of efficiency in the wireless network and above 98% of efficiency in the cloud network. In further research, possibility to identify which programming technique used to store the activity log into the database, identify the performance analysis of algorithm which is opt to implement the intrusion detection and prevention system by using big data even the network is wired or wireless or cloud network.

References

[1] Parag K. Shelke, Sneha Sontakke, Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research, Vol. 1, Iss. 4, May 2012, PP: 67-71.
[2] Amjad Hussain Bhat, Sabyasachi Patra, Debasish Jena, "Machine Learning Approach for Intrusion Detection on Cloud Virtual Machines", International Journal of Application or Innovation in Engineering & Management, Vol. 2, Iss. 6, June 2013, PP: 57-66.
[3] Michal Korcak, Jaroslav Lamer and Frantisek Jakab, "Intrusion Prevention / Intrusion Detection System (IPS/IDS) for Wifi Networks", International Journal of Computer Networks & Communications, Vol. 6, No. 4, July 2014, PP: 77-89.
[4] Shiva rama krishna, Siva Rama Prasad Kollu, Narasimha Raju, "A Comparative Study of Firewall and Intrusion Prevention System", International Journal of Innovative Research in Computer Science & Technology, Vol. 2, Iss. 6, November-2014, PP: 36-39.
[5] Trupti Dange, Pankaj Bhalerao, "A Review of Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", International Journal of Science and Research, Vol. 3 Iss. 11, November 2014, PP: 2373-2377.