First International Conference on Computer Engineering
International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
Volume 5 Issue 8, November-December-2020

Identify the Hacker Using IDS And Prevent the Hacker Using IPS to secure the Cloud Data

Geetanjali Pandey[1], Maithili Gavli[1], Shruti Khaire[1], Pragati Mote[1], Prof. Vandana Chavan[2]

[1]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Maharashtra India

[2]Professor Computer Engineering, Dr. D. Y. Patil School of Engineering Lohegaon, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT

Data-Security generally refers to the protective measures of securing data from unapproved access and data corruption throughout the data lifecycle. It measures not only helps avoid data breaches but also shields your organization against unnecessary financial costs, loss of public trust and potential threats to brand reputation and future profits too. Nowadays, the data is stored in the cloud. Thus, Cloud-Computing is the delivery of different services throughout the internet. These resources include tools and applications like data storage, servers, databases and networking. As long as an electronic device has access to the web, it has access to the data and software programs to run it. Cloud storage technology develops very fast, and cloud storage security technology is facing unprecedented

Challenges. However, cloud storage security is not just a technical issue [5]. Now, in the fifth generation increase in the use of cloud computing, lead to the demand of CLOUD-SECURITY.

Cloud-security have security principles applied to protect the data, applications and infrastructure associated within the cloud computing technology. Thus, we are developing an application to secure the cloud. The evaluation system includes security scanning engine, security recovery engine, security quantifiable evaluation model, visual display module and etc. The security evaluation model composes of a set of evaluation elements corresponding different fields, such as computing, storage, network, maintenance, application security and etc [4].

In order to effectively manage the networks for administrators within limited time and energy, we develop a hierarchical framework which detects the malicious attacks and prevent our data from that attacks. Thus, in our application we are using two algorithms, firstly IDS (Intrusion Detection System) to detect the attack, provide the information of the hacker to the administrator and the second algorithm used is named as IPS (Intrusion Prevention System) to prevent our data from the hacker. We are also going to retrieve the data of the hacker by using support vector machine (SVM).

Keyword—Data security, Cloud-Computing, Cloud security, IDS, IPS, SVM.

I. INTRODUCTION

Capturing and analysing the abnormal behaviour is one of the most critical issues in keeping a network, data centre or cloud under control. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are regarded as the most important techniques in security management [9]. We will develop a hierarchical framework to perform high threat mining and ranking based on their processing urgencies, in turn to reduce the operating difficulties for the network administrators. We have seen that personal computer's data and the cloud data are hacked due to less security provided by the user. This Data and the information is hacked or changed by the hacker, so we need to recover the hacked data or the retrieved data. In the existing system, there is no application to identify and detect the hacker. So in the current system, we use IDS and IPS techniques for detecting and preventing the data from the hacker.

IDS is a system that monitors network traffic for suspicious activity and issues alert when such activity is been discovered. It is a software application that scans the whole network or a system for harmful activity or policy breaching. A good intrusion detection system requirements for the highest possible detection rate and false alarm rate as low as possible due to intrusion detection in user behavior mainly as a data format, so the core problem is how to correctly and efficiently handle the data collected, and reach a conclusion.

An IPS is a system that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. Thus, Intrusion Prevention System is also known as Intrusion Detection and Prevention System

We are also retrieving the cloud data using SVM. SVM is a supervised machine learning algorithm and can be used for both classification and regression challenges. However, it is mostly used in classification problems.

Thus, in the proposed system, we are aiming to provide the security to our data stored in the cloud server, so that we can prevent our data from any malicious activity.

II. LITERATURE SURVEY

Table 1 – Literature Survey

Sr. No	Paper	Remarks
1.	Data Mining Based Intrusion Detection System application	Aimed on operating principle of IDS based on data mining [1].
2.	Design of a new Intrusion Prevention System of application	Introduction of IPS and discuss of the various threats To prevent them [2].
3.	Design of the Intrusion Detection System Based on Multi-Agents in the Ecommerce System	The system structure of IDS based on the Mobile Agent is proposed and then design of the MAIDS system [3].
4	One quantifiable security evaluation model for cloud computing platform	Quantifiable security evaluation system for different clouds that can be accessed by consistent API [4].

5.	Study on Data Security Policy Based On Cloud Storage	This paper is to achieve data security for cloud storage and to formulate the corresponding cloud storage security policy [5].

III. ALGORITHMS

1] IDS (Intrusion Detection System)

In this system we present Genetic Algorithm approach which can efficiently detect the various types of network intrusions. Genetic Algorithm is used to optimize the search of attack and by combining the IDS with genetic algorithm increase the performance of the detection rate of the Network Intrusion Detection Model and reduces the false positive rate. Intrusion Detection System (Intrusion Detection System) IDS surface it looks like network monitoring and alarm devices, a kind of observation and analysis of network attack has occurred, and to send a warning before the attack, and then do a corresponding counter-measures to reduce the huge losses the device may occur[1]. IDS is a system that monitors network traffic for suspicious activity and issues alert when such activity is been discovered. It is a software application which scans whole network or system for harmful activity or policy breaching. It monitors and analyses the user and system activities. It performs auditing of the system files and other configurations of the operating system. It assesses integrity of the system and data files. It conducts analysis of known attacks based on patterns. It detects errors in system configuration. It detects and alerts if the system is in danger. Intrusion detection system for detecting an attempt to undermine the integrity of computer resources, authenticity and availability of software behaviour, it can real-time monitoring system activities, real-time discovery of aggressive behaviour and take appropriate measures to avoid or minimize the occurrence of attacks generated by attack hazard[1].

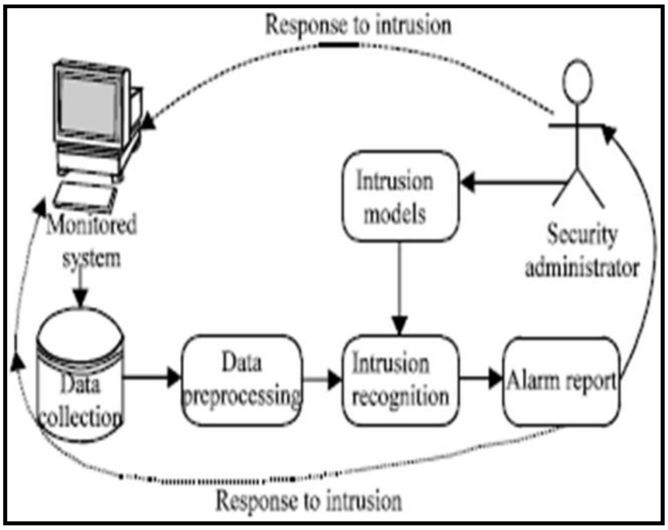

FIG 1 - IDS

2] IPS (Intrusion Prevention system)

An IPS is a system that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. Thus, Intrusion Prevention System is also known as Intrusion Detection and Prevention System. Intrusion Prevention System (IPS) is an important supplementary for security management [9]. Basically an IPS is a firewall which can detect an anomaly in the regular routine of network traffic and then stop the possibly malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it. Intrusion prevention is to detect and identify any abnormal user behaviour which aims at destructing information security and / or stability through the network [2]. Network-based IPSs create a series of choke points in the enterprise that detect suspected intrusion attempt activity. Placed inline at their needed locations, they invisibly monitor network traffic for known attack signatures that they then block. These systems don't reside on the network per se but rather on servers and individual machines. They quietly monitor activities and requests from applications, weeding out actions deemed prohibited in nature. These systems are often very good at identifying post-decryption entry attempts. These IPSs scan network packets, looking for signatures of content that is unknown or unrecognized or that has been explicitly labelled threatening in nature. Intrusion Detection System (Intrusion Detection System)IDS surface it looks like network monitoring and alarm devices, a kind of observation and analysis of network attack has occurred, and to send a warning before the attack, and then do a corresponding counter-measures to reduce the huge losses the device may occur[1].

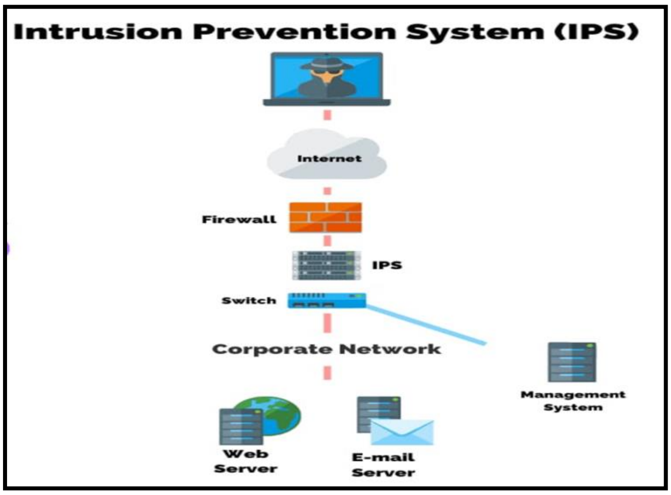

FIG 2- IPS

3] SVM (Support Vector Machine)

SVM is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In the SVM algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiates the two classes very well. SVM's are very good when we have no idea on the data. Works well with even unstructured and semi structured data like text, Images and trees. The kernel trick is real strength of SVM. With an appropriate kernel function, we can solve any complex problem. It scales relatively well to high dimensional data.

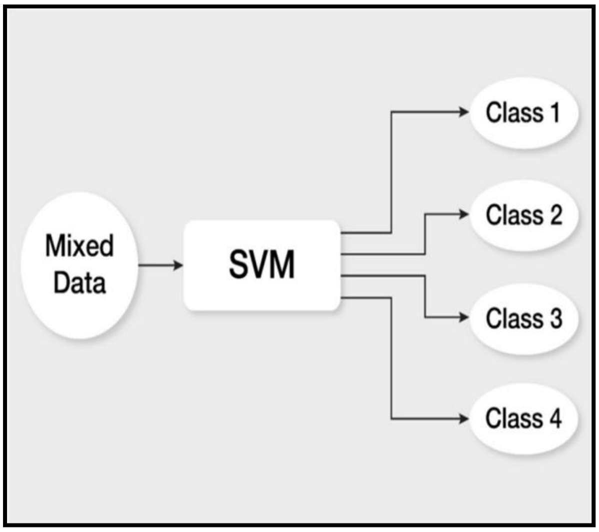

FIG 3- SVM

IV. EXISTING SYSTEM

In existing system there is no computerizes system to identify intrusion detection attack in your personal computer or laptop. A hacker can easily change your personal database or hack our personal database. But we cannot identify them so we can't understand who is stolen our data. So in proposed system we are trying to give security to our data and stored out data in cloud server so hacker cannot identify the data storage location. The existing network intrusion detection research is mostly concentrated on the wired network, the intrusion detection research on wireless sensor networks is relatively little [2].

V. MATHEMATICAL MODEL

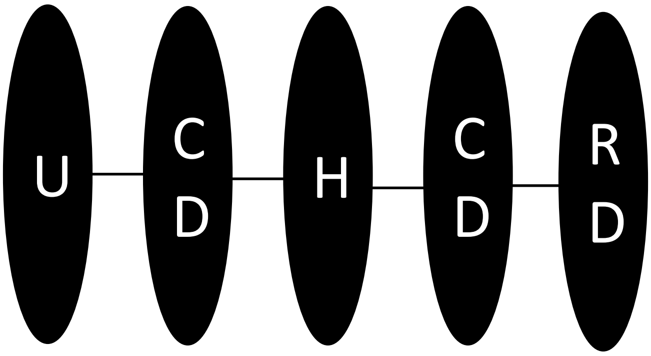

FIG 4 - MODEL

Where,
U =User stores data on Cloud
CD=Data stored on cloud server
H =Hacker can make login attempt
CD =Hacker changes the data
RD =Retrieve the original data.
Above mathematical model is NP-Hard
Because sometime result is not accurate.

Input: Hacker can make login attempt on the user's Pc.
Output: System then captures the hacker's face, retrieve the data and system is blocked.

Let us consider, H as hacker who can make login attempt on user's PC and change the data.
H = {U, CD, CD}
Where,
U = {User can upload data on cloud server.}
CD = {Cloud server store the user's data}
CD = {Hacker can change the data of user}

U = {H, CD, RD}
Where,
H= {User receives hacker's face image via mail}
CD = {Hacker can change the data of the user}
RD = {System data is retrieved which was changed by the hacker}

Functions: Functions implemented to get the businessman original data and detect the hacker face.
Functional relations: 1] Hacking, 2] Security, 3] IPS, 4] IDS.

Success Condition: Successfully algorithm implementation and proper input
Failure Condition: 1. huge data can lead to more time consumption to get the information.2. Hardware failure.3. Software failure.

Space Complexity: The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity.
Time Complexity: Check No. of patterns available in the database = n. If (n > 1) then retrieving of information can be time consuming. So the time complexity of this algorithm is O (n ˆn).

VI. SYSTEM ARCHITECTURE

If hacker is trying to hack the data of our system , we will catch the face of the hacker if login attempt fail at the first time.In the second time if attacker changed the data on our PC, then our system will retrieve the previous data using support vector machine. If the hacker attempted for the third time to hack the system then we will block the system, and we will not provide any login option for the hacker.

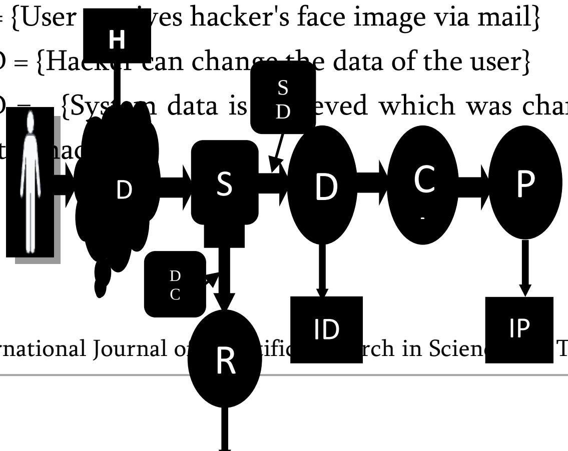

FIG 5 – SYSTEM ARCHITECTURE

VII. Advantages of System Architecture

[1] Using IPS and IDS algorithm system can provide the security to the user's important information and data.

[2] SVM algorithm can recover the user's important information and data which is changed or modified by the hacker.

[3] This is reliable system.

[4] This system can prevent the hackers from hacking.

[5] When hacker trying to hack the user's important information and data then system send the email of the hacker's image to user, because of this email system immediately alert the user.

[6] Replace a Human Monitoring Your Network 24x7.

VIII. APPLICATIONS

[1]. Small business: The reason being, many large companies have the infrastructure in place to guard against cyber-attacks. Small businesses, however, either don't have the proper resources to thwart an attack or they don't take cybersecurity as seriously as they should.

[2]. Healthcare: The healthcare industry is another prime target for ransomware attacks because of the sheer amount of patient data stored by healthcare entities. Health information is some of the most valuable data on the dark web because it can be used to commit insurance fraud.

[3]. Higher Education : When you think of potential targets for hackers, colleges and universities probably aren't the first to come to mind, however, the higher education industry is another mecca of personal data. From social security numbers, addresses and passwords to loan and bank information, it's no wonder attacks on colleges and universities are becoming more prevalent.

[4]. Energy: Last, but by no means least, is the energy sector. Here, things like the electric power grid and power generation facilities are controlled by technology and communication systems that could be disrupted, hacked or taken over during a cyber-attack to put our economy in serious danger.

IX. CONCLUSION

In order to effectively manage the networks for administrators within limited time and energy, we develop a hierarchical framework to secure the data of the user by detecting and preventing any malicious attack. With the help of IDS and IPS our data is highly secure. We can also get image of the person who is unauthorized accessing our data. If our data is hacked then we can also retrieve it. We can also block the system if hacker is repeatedly trying to attempt the login. Thus, we find that the accuracy of our proposed method is larger than 97%, the analysis results verify that our proposed methods is more effective compare with other methods[9].

X. FUTURE WORK

[1] Malware targeting virtual machines: "Many breeds of malware today can detect if they are running within virtual machines and make

adjustments or shut down altogether in order to evade detection, but only a few proof of concept viruses have actually attempted to break free into the host machine," explained Fred Couchette, senior security analyst at Approvers. "We expect to see more of these in the near future."

[2] ATM-like hardware hacks: "We've seen criminals physically walk in to stores and replace credit card terminals with working replacements that had been modified to contain a 3G modem, which transmitted payment details directly back to them," said Lyne. "This high scale, intelligent hardware hacking demonstrates that the threat is not just impacting the conventional PC."

[3] RAM scraping: "For years everyone has been locking down databases since they are the source of information, but now hackers that can breach a server can get an application less than 1MB in size on the server and capture all the data as it is written to RAM before it goes to a database," said Chris Drake, CEO of Fire Host. "An application like this can also capture data (such as credit card numbers) that don't even go into a database, but that are processed by a third party provider. RAM scraping will be a huge concern as it gains more popularity among the hacker crowd.

XI. REFERENCES

[1]. FAN Yaquina College of Communication. Engineering, Jilin University Changchun 130012, china fanyaqin_joy@163.com, Paper Name- Data Mining Based Intrusion Detection System in VPN Application.

[2]. Huangzhong Hua School of Mechatronical Engineering Beijing Institute of Technology Beijing China fengqingjuan@foxmail.com, Paper Name- Design of a new Intrusion Detection System of WSNs.

[3]. Yabo Li College of Business Administration of HUNAN University lyb412@sina.com, Paper Name- Design of the Intrusion Detection System Based on Multi-Agents in the Ecommerce System.

[4]. Aobing Sun1,2* , Guohong Gao1 , Tongkai Ji1,2 , Xuping Tu1,2, Paper Name-One quantifiable security evaluation model for cloud computing platform.

[5]. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan University of International Relations, Beijing, China, Paper Name-Study on Data Security Policy Based On Cloud Storage

[6]. Salah S, Maciá-Fernández G, Díaz-Verdejo J E, "A model-based survey of alarmcorrelation techniques," Computer Networks, vol. 57, pp. 1289- 1317, 2013.

[7]. Dwivedi, Neelam, and A. Tripathi, "Event Correlation for Intrusion Detection Systems," IEEE International Conference on Computational Intelligence & Communication Technology IEEE, pp. 133-139, 2015.

[8]. Zhang S, Gao Y, Zhang M, et al, "The Study of Network Security Event Correlation Analysis Based on Similar Degree of the Attributes," Digital Manufacturing and Automation (ICDMA), pp. 1565-1569, 2013.

[9]. Yongwei Meng. Tao Qin, Member, IEEE. Yukun Liu, Student Member, IEEE and Chao He.Paper Name-An Effective High Threating Alarm Mining Method for Cloud Security Management.