International Conference - Innovation-2021-Innovation-2021
International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)
Volume 8, Issue 3, May-June-2021

Quantifiable Data Security Model for Cloud Computing Platform

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

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

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

ABSTRACT

Whatever one public cloud, private cloud or a mixed cloud, the users lack of effective security quantifiable evaluation methods to grasp the security situation of its own information infrastructure on the whole. This paper provides a quantifiable security evaluation system for different clouds that can be accessed by consistent API. 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. In order to effectively manage the networks for administrators within limited time and energy, we are developing a hierarchical framework which detects the malicious attacks and prevent our data from that attack. Thus, in our application we are using two algorithms, firstly Intrusion Detection System (IDS) which is used to detect the attack and provide the information of the hacker to the administrator and the second algorithm used is named as Intrusion Prevention System (IPS) to prevent our data from the hacker. We are also going to retrieve the data which are changed by the hacker using support vector machine (SVM).

Keywords: Cloud-Computing, Security, IDS, IPS, SVM.

I. INTRODUCTION

With the continuous development of cloud computing technology, cloud has become one common method to create the different users' information infrastructure [1]. But as the cloud technology brings us very low-cost services and operation conveniences, it also caused that the information infrastructure of users is fragmented. The cloud users cannot know whether their cloud services are safe, and whether their data can be safely placed in different clouds. Currently, capturing and analysing the abnormal behaviour is one of the most critical issues in keeping a network, data centre or cloud under control. Firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are regarded as the most important devices for security management [2]. 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 [3].

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 [4].

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 [5].

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

Sr. No	Paper	Remarks
1.	One quantifiable security evaluation model for cloud computing platform	Aimed on quantifiable security evaluation system for different clouds that can be accessed [1].
2.	An Effective High Threating Alarm Mining Method for Cloud Security Management	Introduction of IPS and IDS discuss of the various threats to prevent them [2].
3.	Data Mining Based Intrusion Detection System in VPN Application	Quantifiable security evaluation system for different clouds that can be accessed by consistent API [3].
4	Design of a new Intrusion Detection System of WSNs	In this paper a new Intrusion Detection System of WSNs is designed, its detection work is based on selective available information of every node in the network [4].
5.	A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS)	IDS will identify the internal intruder's accurately in real time and can be used by several firms, MNC's for protecting their valuable data. [5].
6	Study on Data Security Policy Based On Cloud Storage	The purpose of this paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy.
7	Distributed Intrusion Detection System using Block chain and	Proposes the development of Distributed Intrusion Detection System (DIDS)

	Cloud Computing Infrastructure	
8	Intrusion detection systems vulnerability on adversarial examples	The role of Intrusion Detection System within security architecture is to improve a security level by identification

Table No .01

III. ALGORITHMS

1]. IDS (Intrusion Detection System)

Intrusion detection system (IDS) is a system that monitors and analyses data to detect any intrusion in the system or network. High volume, variety and high speed of data generated in the network have made the data analysis process to detect attacks by traditional techniques very difficult. 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]

The IDS has three methods for detecting attacks; Signature-based detection, Anomaly-based detection, and Hybrid-based detection. An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates the outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

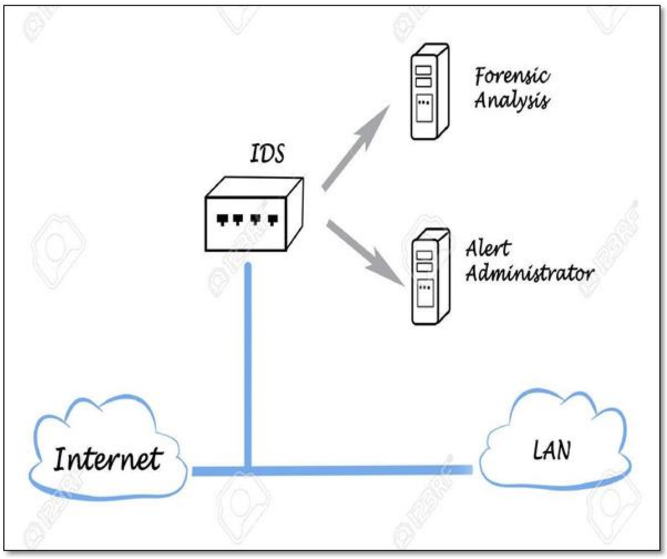

FIG 1. IDS

2]. IPS (Intrusion Prevention system)

Intrusion Prevention Systems are an important component of IT systems, defence, and without this technology, our data and our networks are much more susceptible to malicious activities. Intrusion Prevention Systems, a more advanced version of Intrusion Detection Systems, are now making their mark on the IT industry reaching a new level of network security. An IPS (Intrusion Prevention System) is any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. 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.

Intrusion Prevention System (IPS) is an important supplementary for security management [9]. There are many reasons why someone would want to use an IPS, among these are extra protection from denial of service attacks and protection from many critical exposures found in software such as Microsoft Windows. The capabilities of IPSs are already in use by large organizations and in the near future we will more than likely see private home users utilizing a variation of IPS. IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.[4]

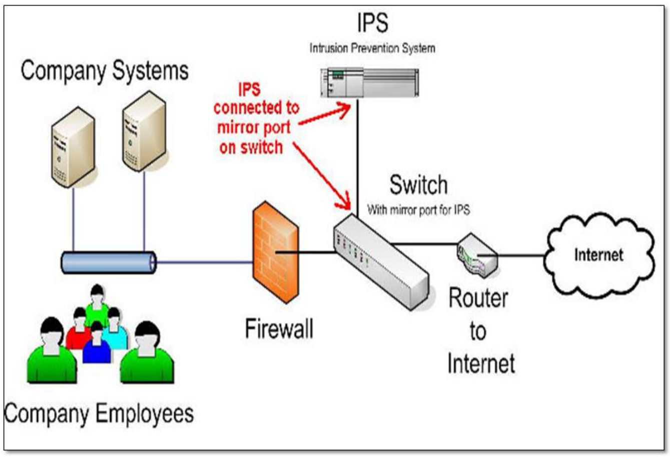

FIG 2.IPS

3]. SVM (Support Vector Machine)

The objective of the support vector machine algorithm is to find a hyper plane in an N-dimensional space (N — the number of features) that distinctly classifies the data points. An SVM model is basically a representation of different classes in a hyper plane in multidimensional space. The hyper plane will be generated in an iterative manner by SVM so that the error can be minimized. The goal of SVM is to divide the data sets into classes to find a maximum marginal hyper plane (MMH). The followings are important concepts in SVM – 1.Support Vectors – Data points that are closest to the hyperplane is called support vectors. Separating line will be defined with the help of these data points.

2. Hyper plane – As we can see in the above diagram, it is a decision plane or space which is divided between a set of objects having different classes.

3. Margin – It may be defined as the gap between two lines on the closet data points of different classes. It can be calculated as the perpendicular distance from the line to the support vectors.

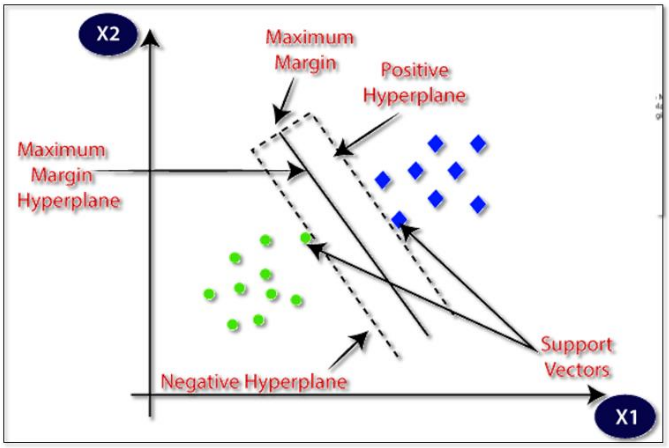

FIG 3. SVM

IV. EXISTING SYSTEM

In the 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 has stolen our data. So in proposed system we are trying to give security to our data and stored out data in a 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

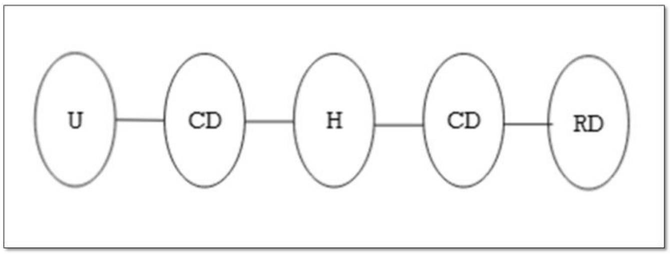

FIG 4. MODEL

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 consuming 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 a hacker is trying to hack the data of our system, we will catch the face of the hacker if a login attempt fails at the first time. At 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.[10]

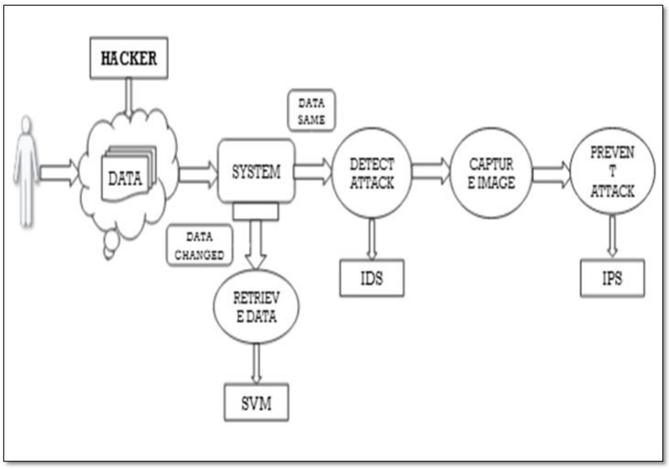

FIG 5. SYSTEM ARCHITECTURE

VII. IMPLEMENTATION

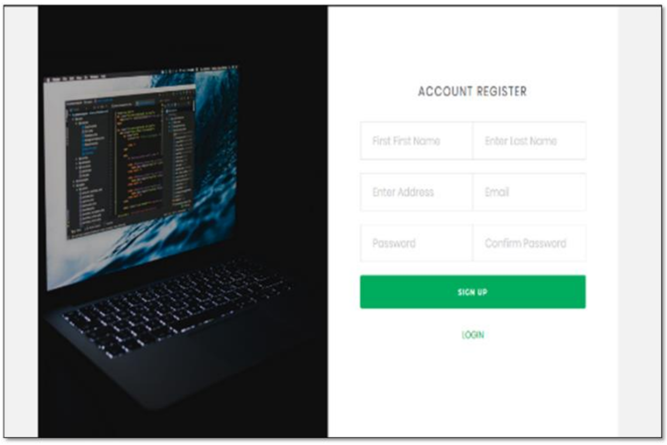

FIG 6. REGISTER PAGE

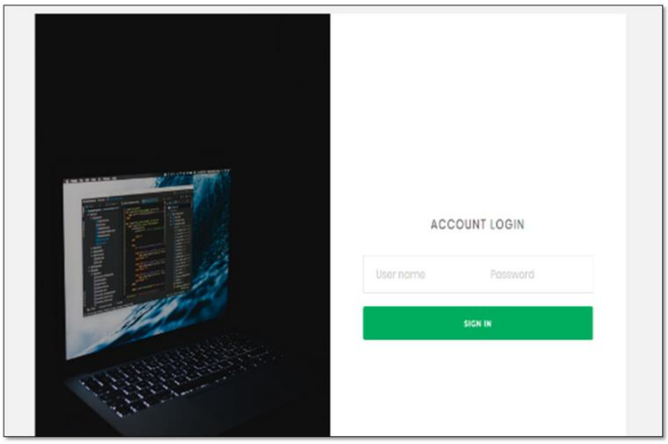

FIG 7. LOGIN PAGE

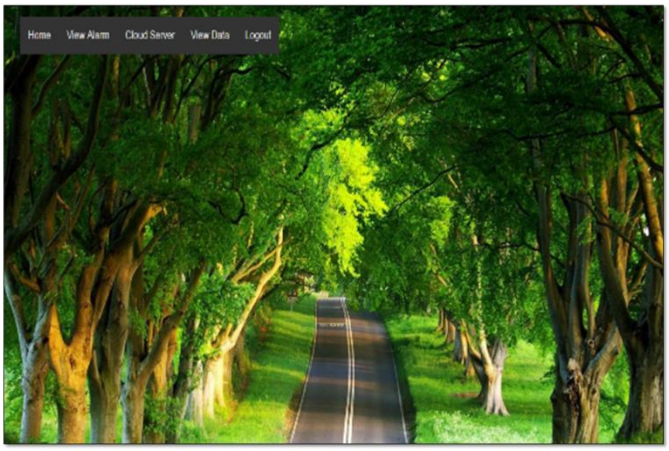

FIG 8. HOME PAGE

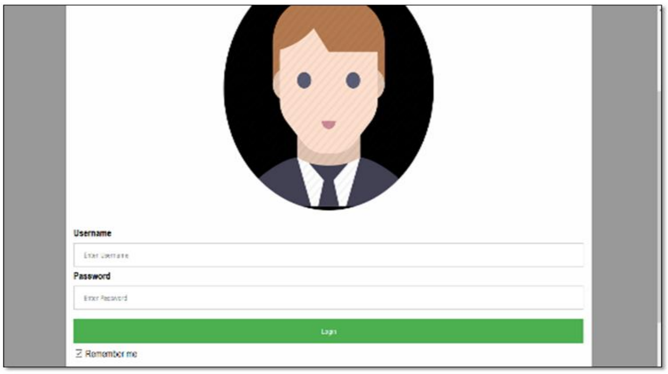

FIG 9. CLOUD LOGIN

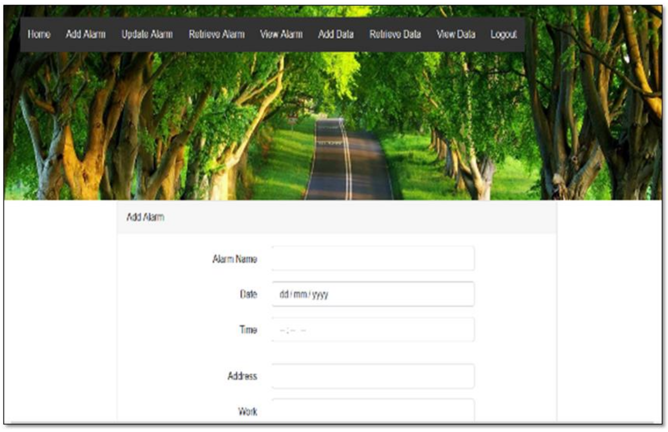

FIG 10. CLOUD DATA

VIII. ADVANTAGES OF SYSTEM ARCHITECTURE

1]. Using IPS and IDS algorithm system can provide the security of 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 the user, because of this email system immediately alerts the user.

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

IX. APPLICATIONS

1]. Small business: The reason being, many large companies have the infrastructure in place to guard against cyberattacks. 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 cyberattack to put our economy in serious danger.

X. 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 images 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 compares more effectively with other methods[9].

XI.FUTURE WORK

1]. Malware is 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 has 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 into stores and replace credit card terminals with working replacements that had been modified to contain a 3G modems, 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 is scraping: "For years everyone has been locked 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 into 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.

XII.REFERENCES

[1]. Mohan Sundaram, R., A. Jayanthiladevi, and G. Keerthana. "Software Defined Cloud Infrastructure." Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science. IGI Global, 2018. 108-123.

[2]. Rittinghouse, John W., and James F. Ransome. Cloud computing: implementation, management, and security. CRC press, 2016.

[3]. Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6.1 (2014): 25.

[4]. Carlin, Sean, and Kevin Curran. "Cloud computing security." (2011)

[5]. Gouda M, Liu X, "Firewall design: consistency, completeness, and compactness," In Proceedings of the 24th IEEE International Conference on Distributed Computing System, 2004.

[6]. Valeur F, Vigna G, Kruegel C, et al, "A Comprehensive approach to intrusion detection alarmcorrelation," IEEE Transactions on dependable and secure computing,vol. 1, pp. 146-169, 2004.

[7]. Kumar S, Spafford E H, "A Software Architecture to support Misuse Intrusion Detection," Computers & Security,vol. 14, 1995.

[8]. Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, et al, "Anomalybased network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, pp. 18-28, 2009.

[9]. Lee, Texas, Deng Xiaohui. Network virus against the status quo and Countermeasure technology. Network Security Technology Operation and applications, 2001,8 (2) :96-100

[10]. Wu occasion, Huang Chuan-he, WANG Li-Na and so on. Based on data mining intrusion detection system. Computer and Applications, 2003,10 (4) :48-54