International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9794-9801

Integrated Approach to Cloud Security: IACS

Vimmi Pandey[1, 2,*], and Dr. Mridula Dube [2]

[1]Rani Gurgavati Vishwavidyalaya, Jabalpur, Madhya Pradesh, India.
[2] Rani Gurgavati Vishwavidyalaya, Jabalpur, Madhya Pradesh, India.

Abstract—

Security over cloud has been challenging for the researchers and they have been providing good solution. But growth in technology is imposing new challenges and to tackle these, better solution is needed always. This paper proposes and implements an integrated approach to solve multiple security issues simultaneously. This approach will help the cloud system to handle many security issues using a single solution. This work proposes to use IDS, a Trust server and access control along with the encryption and decryption of the various data being used over the cloud. Having such a solution will be able to cope up with the various security problems such as man in the middle attack, DoS, malicious users and fishing attacks etc. This work is being implemented using the case study of shopping cart for a book seller and various results obtained there in are presented to provide the correctness of the proposed solution.

Keywords: Cloud Computing, Security, Intrusion Detection System, Alarming System, abnormal behaviours, Masquerade.

INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it.

The cloud is emerging as the latest way to approach alternative delivery models for IT capabilities. It is a way of delivering IT- enabled services in the form of software, infrastructure and more. This research examines the definition of cloud computing and how it will evolve. [11]

Cloud computing can be defined as "A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing platforms on demand, which could be accessed in a simple and pervasive way"[12]. In simple words, Cloud computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Cloud computing aims to provide scalable and inexpensive on -demand computing infrastructures with good quality of service levels. Cloud Computing is the implementation of engineering principals to obtain high quality applications through Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [13].

Cloud computing provides the internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model is introduced by NIST [14] as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter [15]. Cloud computing can be divided into two sections, the user and the cloud. In most scenarios, the user is connected to the cloud via the internet. It is also possible for an organization to have a private cloud in which a user is connected via an intranet. However, both scenarios are identical other than the use of a private and public network or cloud [16]. The user sends requests to the cloud and the cloud provides the service.

During the past few years, the number of intrusions in computer networks has grown extensively, and many new hacking tools and intrusive methods have appeared. Using IDS is one way of dealing with suspicious activities within a network [1].The intrusion behaviours cause the great damage of systems. So enterprises search for intrusion detection systems to protect their systems. The traditional technology such as firewall is used to defence attacks.

Thus, the IDS usually used to enhance the network security of enterprises. The major difference between firewall and IDS system is that firewall is a manual passive defence system.

Comparatively, IDS could collect packets online from the network. After collecting them, IDS will monitor and analyze these packets. So, IDS system acts as the "second line of defence". Finally, it will provide the detecting results for managers. The detecting results could be either attack or normal behaviour. An ideal IDS system has a 100% attack detection rate along with a 0% false positive rate, but it is hard to achieve. Detecting illegal behaviours of the host or network is the major object of IDS. The IDS is actually such a system to detect some illegal behaviour.

One of the ability of IDS is it could monitor various activities on the network. IDS will send a warning message to the managers if it detects an attack.

Briefly, the aim of IDS is to detect intruders or attacks effectively [2]. There are two main methods of IDS, misuse or

signature detection and anomaly detection.

Signature or Misuse Detection is known intrusions are detected by looking at the computer system behaviour some characteristic pattern of such intrusions. This approach uses some collected information about the system behaviour under normal conditions and under some known intrusions to determine the current state of them system. In this case, the intrusion detection problem is a classification problem [3].

Misuse detection refers to techniques that characterize known methods to penetrate a system. These penetrations are characterized as a 'pattern' or a 'signature' that the IDS look for. The pattern or signature might be a static string or a set sequence of actions. System responses are based on identified penetrations. The idea of misuse detection is to establish a pattern or a signature form so that the same attack can be detected. The other idea here is to establish a normal activity profile for system. False alarm rate refers to the proportion that normal data is falsely detected as attack behaviour, namely a false positive (FP) situation. Accuracy is defined as the proportion of data correctly classified that is a true positive (TP) and true negative (TN) [4].

Cloud computing is an efficient technology to improve the performance of organizations by providing flexibility in architecture and reduction in costs. Dynamic resource pooling, virtualization, on demand service and high availability are some of the advantages provided by cloud computing. However, open and distributed architecture as well as internet access, have caused cloud environments to be risky and vulnerable. Privacy, confidentiality, and authentication are some of security concerns which need to be addressed. Authors propose a secure mechanism for authentication and session key distribution. For this purpose, they have chosen Kerberos 5 protocol that is one of the best known authentication and key distribution systems. But, this protocol is vulnerable to password guessing attack. Hence, they improve the Kerberos 5 with Strong Diffi-Hellman-DSA key exchange algorithm and the user's fingerprint samples. This approach provides a protocol which is highly secure. Authors solve the password guessing attack vulnerability using Strong Diffi-Hellman-DSA Key Exchange algorithm. Also, the use of biometric data provides a non-repudiation mechanism that can address the limitation of password-based authentication, such as the tendency of users to choose a simple password. In addition, we implement this scheme in cloud computing systems and use an enhanced approach for fingerprint template protection. [5]

The era of cloud computing has brought with it several new methodologies to use the smart devices and objects in our day to day life paving its way towards the Internet of Things (IoT) cloud networks. This enables the use of embedded technology which in turn helps it to easily interact and share information with the external environment by the help of internet. Despite all the positive influence that the IoT cloud network has garnered since its arrival, one cannot simply rule out the risks that accompany this technology which turns out to be a hindrance in its adoption. Security issues in IoT cloud networks are especially concerned with the communication security and end-user privacy protection. In this scenario there is always a possibility that a non-malicious user may share the same network as a malicious user. The traffic generated by a malicious user can cause a degradation in the performance of other sensors and can also cause erroneous billings when it comes to other nodes in t he virtual network [6]–[8]. The cloud service provider (CSP) plays an important role in monitoring and controlling the traffic generated by various IoT nodes. There are various issues that make traffic management a headache for the CSP such as confidential information of a usergroup is not to be shared with the CSP and the CSP has to support IoT nodes mobility which makes traffic management a very cumbersome task [7]. The basic idea behind the work is to establish a secure communication between the cloud service provider and the IoT nodes that are placed within different user groups in different virtual networks. There exist a communication between the cloud service provider and the user groups over a public channel. The user groups are thus assigned tasks among themselves by the CSP. There can also be an instance where the IoT nodes placed in one user group would like to communicate with different IoT nodes placed in other user group in different virtual network; this particular communication among the CSPs and user groups may be intercepted while they are being transmitted over a public channel. Thus the proposed architecture provides a key management policy of the IoT nodes using BIBD (Balanced Incomplete Block Design) approach where the key is distributed from a key pool by the CSP to the different user groups over a secure communication channel [9]. The distributed valid keys are further taken into consideration for a lightweight cryptographic encryption and decryption in order to establish a secure end-to-end communication among the IoT nodes in their respective user groups [10].

ISSUES IN CLOUD DATA STORAGE

Cloud Computing moves the applying software system and information bases to the big data centres, wherever the management of the information and services might not be totally trustworthy. This distinctive attribute, however, poses several new security challenges that haven't been well understood. In this, we tend to target cloud information storage security, which has invariably been a very important side of quality of service to make sure the correctness of users' information within the cloud.

A. Trust:

B. Privacy

C. Security

D. Ownership

E. Performance and Availability

A. CHARACTERISTICS OF CLOUD COMPUTING

1. Broad network access

2. On-demand self-service

3. Location Independence Customer

4. Resource pooling

B. SECURITY ISSUES AND RISKS IN CLOUD COMPUTING

Gartner in 2008 recognized seven security issues [17] that need to be tended to before organizations switch completely to the cloud computing model.

1. Data location

2. Regulatory compliance

3. Recovery

4. Privileged user access

Risks in Cloud Computing

The six special areas of cloud computing where substantial security attention is required is are as follows

1. Security of data in transit.

2. Security of data at rest.

3. Cloud legal and regulatory issues.

4. Robust separation between data belonging to different customers.

5. Authentication of users/applications/processes.

6. Indecent response.

C. SECURITY ATTACKS IN CLOUD COMPUTING

While moving from traditional computing paradigm to cloud computing paradigm new security and privacy challenges has emerged. Security of the cloud computing system can be thought in two dimensions: physical security and cyber security.

Physical security concerns the physical properties of the system. For example, a data center, which is owned by provider infrastructure, has to realize security standards and hold security certifications globally, supervision and manageability on security preventions, incombustibility, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) are indispensable [18].

In this section mostly known attack types are detailed.

Insider Attack: Employee, entrepreneur and associates which are still or former attended who can or could access the whole information system with privileged authority are defined as insider [19, 20]

User to Root Attacks: In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system [21].

Attacks on Virtualization: Multiple virtual machines use the same resource pool, especially hardware and with this kind of access side channel data has a chance to be captured, which flow one virtual machine to other [22].

Authorization, Authentication, Encryption, Key and Identity Management: Different from conventional information technologies, in cloud computing deployment of virtual machines, IP addresses and resources are dynamic [23].

Data Modification, Forgery and Integrity: Un-trusted providers and system administrators can manipulate users' and consumers' data among to their own benefits [24, 25, and 26].

Intrusion detection systems (IDS)

An Intrusion Detection System (IDS) is a system that is responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized occurring on a network. An IDS captures and inspects all traffic, regardless of whether it's permitted or not. Based on the contents, at either the IP or application level, an alert is generated.

Four different types of attacks have been identified which makes the need for an IDS critical.

a. Denial of service

Network-based denial-of-service [1, 2, and 3] attacks are one of the easiest types of attacks. It often requires little effort to fully consume resources on the target computer, to starve the target computer of resources, or to cause critical services to fail or malfunction. Internal corporate networks typically do not have internal filtering defences against common denial-of-service attacks, such as flooding.

b. Threat to Confidentiality

Some viruses attach themselves to existing files on the system they infect and they send the infected files to others. This can result in confidential information being distributed without the author's permission. [1, 2, 4, 7, 8]

c. Modification of contents

Intruders might be able to modify news sites, produce bogus press releases, and conduct other activities, all of which could have economic impact. [1, 2, 9, 10]

d. Masquerade

A masquerade takes place when one entity pretends to be a different entity. [1, 2, 11, 12]

The consequences of the attack may vary depending on the system; however, the attack itself is fundamental to the TCP protocol used by all systems.

CASE STUDY

We are creating a login based service for the e-book mart. Here users will be registering themselves as Customer / Resellers for book mart. They will be getting advantage for being Reseller.

When a user will be logging in then he will get a key, which will be used as login credential along with username and password. The admin of the web app shall authorize the user after verification of his details.

The complete process shall be as follows:

1. User will register and be authorized.
2. User will get a key from the trust server via cloud whenever he will login. The key will vary for every login.
3. The key will be used whenever the user will perform any request to the cloud, where cloud will verify the key from the trust server every time. This process will be done by USA.
4. There will two or more servlets running in the background as VMs where only one of the VM will provide services to one user.
5. When VM will be crashing or overloaded then a task migration will be applied, which will not only migrate the VM of app but will also migrate the session key on other server.

IACS is being proposed to handle multiple security issues simultaneously using a single solution and the complete working of the system has been described in following diagram . The system is consisting of different modules and each module contributes not only to provide the required services by it but will also help in enhancing the security over the cloud. The Major modules and their description in sequence is as follows:

Module 1: Application running on the cloud. For the implementation and depicting the proposed system, case study of online shopping cart has been taken for a book seller. The application will have internal service provider sub modules to interact with the different parts of the cloud and other modules. Application will be allowing users and administrator to buy and add books with high security over the cloud.

Module 2: Authentication Services, This module has been developed to implement high level of authentication for the users of the system which includes the buyers (users) and administrators both. User Management has been done to include user email as the user name to provide uniqueness and an encrypted password for managing the password protection from the administrators and other applications running on the cloud. It will also safe guard the users interest from the cloud service provider i.e. confidentiality.

PROPOSED WORK

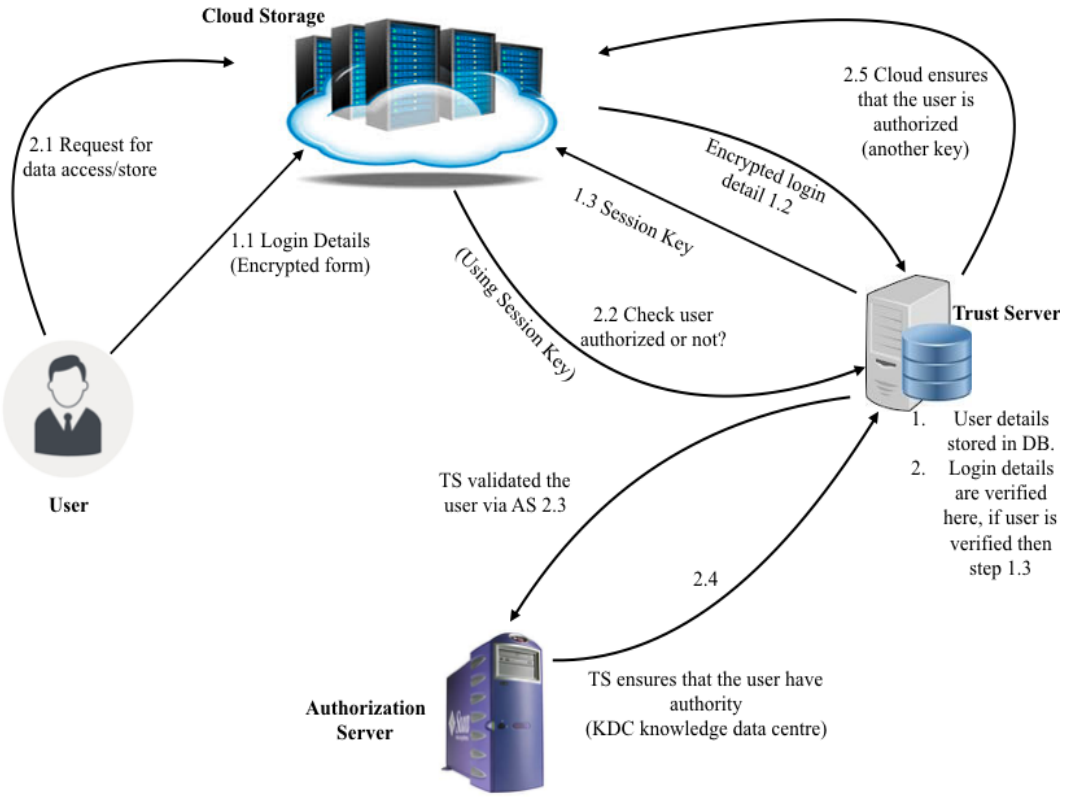

Figure 1: Proposed Methodology

Module 3: IDS, Intrusion detection system is becoming a basic need of the cloud to provide the safety from Denial of Service (DoS) attack, integrity and availability of the system. IDS is an independent module integrated on server for tracking the malicious users and generate alarming for the same. A system has been developed in IACS to tackle with the false alarming by providing blocking and allowing users by the owner account.

Module 4: Trust Manager Module, it is a server application which will handle all the incoming and outgoing requests and responses respectively. It will provide the server based coordination between the different modules of the proposed work. Trust Manager will ensure the trust of the request making users before providing any services to it. For surety of the trust it will use authentication server and authorization servers and knowledge data centre.

Module 5: Authentication Server, This will manage the authentication of the user through encryption and decryption services. For this implementation, One Time Padding (OTP) encryption and decryption algorithm is being proposed which will use key based authentication system. This will interact with trust server only.

Module 6: Authorization Server, This module is also implemented to provide an authorization service for sales made by the system. It will be administrators' description to allow the sale of a book or as per the proposed system.

Alongwith these the use of JAVA languages with latest client side technologies adds to the security for handling attacks such as man in the middle attack, fishing, session high jacking, cross site scripting, SQL injection etc.

RESULTS & DISCUSSION

The proposed system has been developed using an integrated approach proposed in the above section and case study of online book mart. The implementation has been done to map the online shopping cart in such a way so that it will not use a payment gateway and books will be purchased by the customers through the proposed security algorithms. The integrated modules have been developed individually and results obtained from them are as follows:

1) IDS & Alarming System:

The Alarm is generated as follows:

N – Total number of hits in 1 min

N_{IP} – Total of number of different IPs

N_{avg} – Average number of hits per IP Address in 1 min

$N_{Threshold}$ – Threshold set to declare an IP address to be threat

$Navg = N / N_{IP}$

The algorithm used for evaluating the threats and generating alarm are listed in the below boxes. Another algorithm used to count the IPList and Packet Count is also enlisted below.

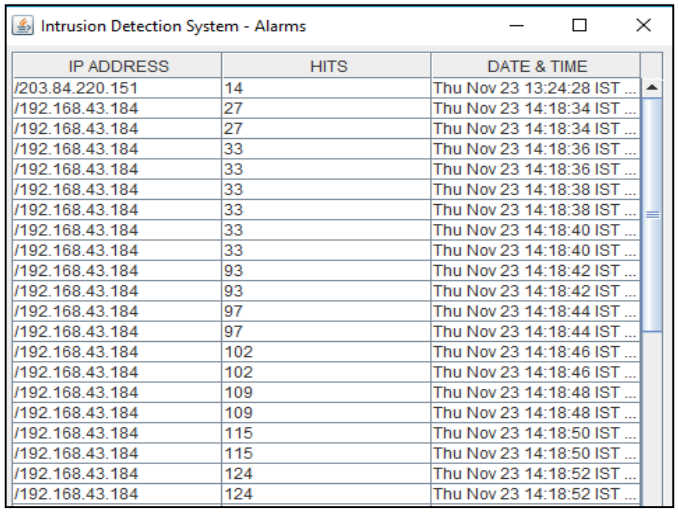

Figure 1. Screen shot of implementation Alarms file being generated for the users.

List of alarms generated and logged in a separate file for future reference. This list can be used as a feedback for improving the security of the system and IDPS implemented.

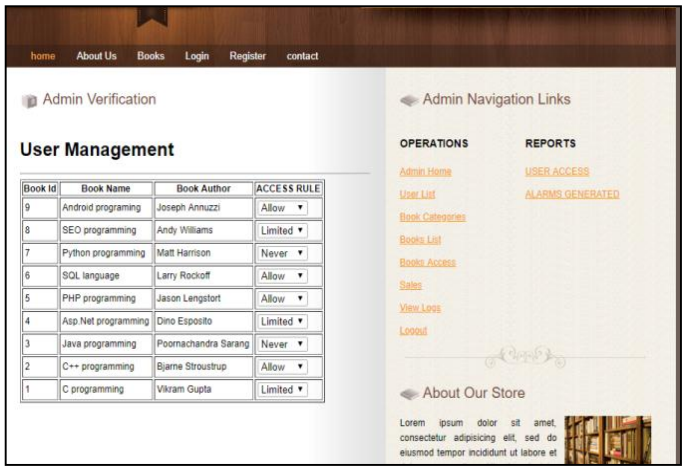

Figure 2. Screen shot of implementation Alarms file being generated for the users.

List of alarms generated and logged in a database table for future reference. This list can be used as a feedback for improving the security of the system and IDPS implemented. It even allows for applying security firewall blocks to the unknown users accessing the system and might be trying for DoS.

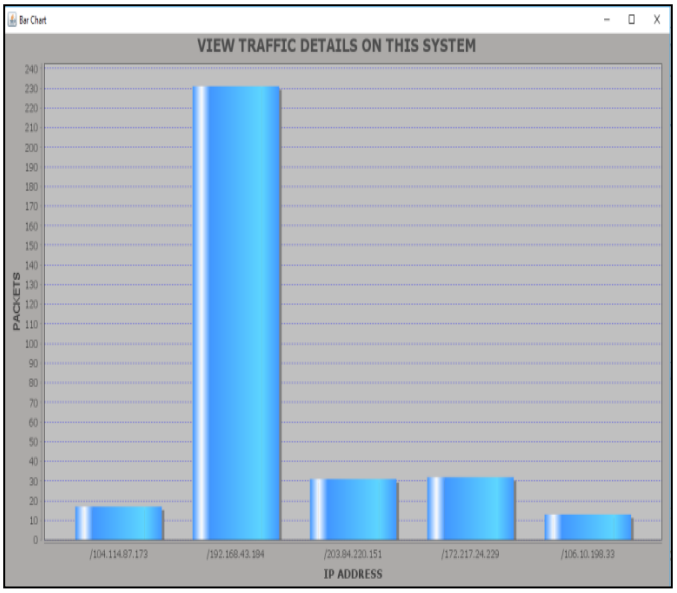

Figure 3. Screen shot of implementation showing graph of the IPs tracked and alarmed for the users.

Graphical representation of the IP Address hitting the system shows how many hits are being done by a particular IP on the system. The IP Address alarming in this work has been implemented using the frequency pattern of the IP Addresses which are hitting the system in per unit time. The Alarm is generated as specified in the starting of the section.

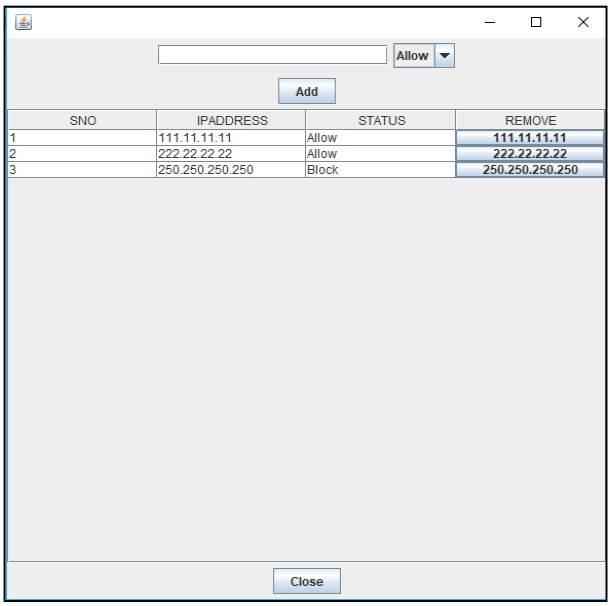

Figure 4. Screen shot of implementation showing IP Addresses to be blocked or allowed for communication through the IDS

List of the IP Addresses added by the user for blocking and allowing. The allow option is for those IP Addresses which are by default blocked by the firewall or antivirus software on the system. Blocked IP Addresses will not be allowed to pass through the system and hence system can be made secured.

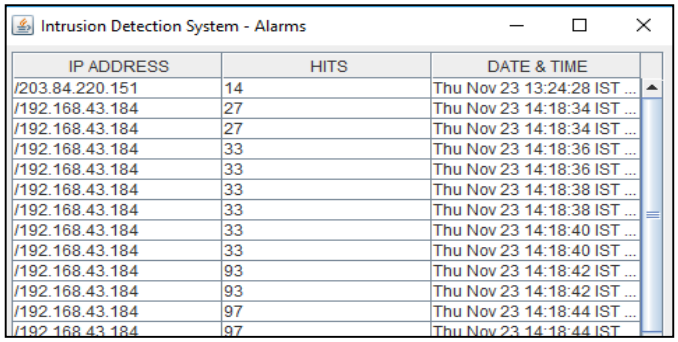

Figure 5. Screen shot of implementation Alarms file being generated for the users.

List of alarms generated and logged in a separate file for future reference. This list can be used as a feedback for improving the security of the system and IDPS implemented.

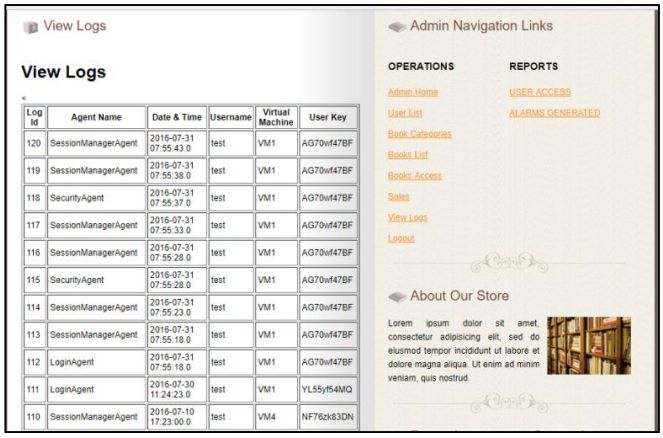

Figure 6. Screen shot of viewing the system logs

The log created above helps in finding the various activities happening on the system and also allows performing necessary preventive actions such as blocking or unblocking the users, generating reports for user actions being done in the system for audits.

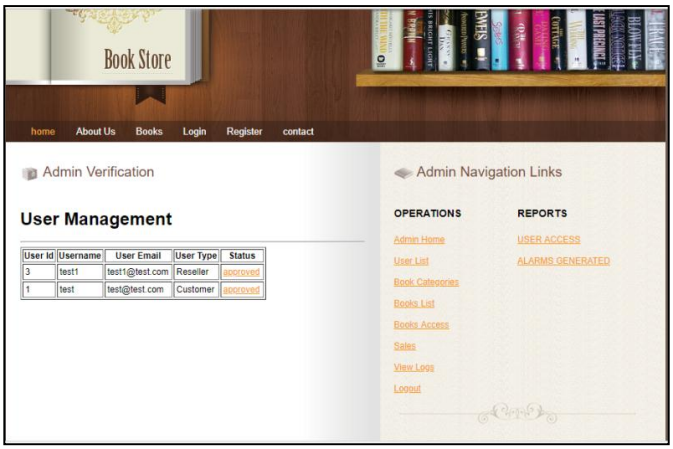

Figure 7. Screen shot for managing user login from list

List of users allows having the quick go through from the users, using the system. It also allows for approving or disapproving the users from the system login and authentication is failed on disapproval.

Figure 8. Screen shot of graph showing the different actions being taken by number of users.

Above image will be useful to control the actions being taken by the user on the system. If the multiple login attempts are shown here then previous list can be used to refer and find the mal performing users of the system.

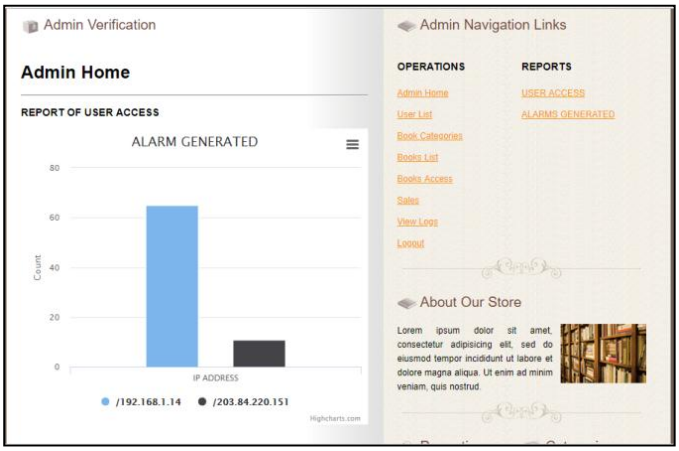

Figure 9. Screen shot of the graph showing the number of alarms generated for specific IPs.

If there are many occurrences of alarming then it is suitable to select the IP Address from the above group and apply the necessary action to block the mal functioning IP Address.

CONCLUSIONS

Integrated approach of Cloud security is helpful in protecting a cloud from multiple threats using a singl platform. It applies intrusion detection system, encryption and decryption, authentication and authorization, trust management using access control, high performance due to work distribution on different servers etc. Many security algorithms and techniques have proposed and implemented over the cloud. This work has proposed and provided an implementation to have a cloud environment applied with the multiple norms to prevent threats quickly with high performance and accuracy. Security of the data of the users of the Cloud is a mandatory requirement and the factors involved in security threats are too many. For achieving security compromise is done in the performance of the cloud services because each packet requires going through a security mechanism involved. This opens the various research gates for achieving high security and performance both. The same can also be used on Virtual Machine Level or server level depending upon the requirement of the system.

Implementation findings are that such a system is highly reliable and able to mitigate all possible threats with certain modifications/additions based on the threat taken in question. It is also found that the system is working efficiently and accurately to the expectation.

In future this work shall be enhanced security based distribution of the task and in other way we can implement more number of threats protection required by the users of the system.

REFERENCES

[1] Dong S, Malcom I& Zinchir-Heywood A.N. 2005."Training Genetic Programming on Half a Million Patterns: An Example from Anomaly Detection", IEEE Transactions on Evolutionary Computation.Vol.9 No.3, pp.225-239,

[2] Vaibhav G,Csill F & Valtorta M, “Paid: A probabilistic agent-based intrusion detection system”. Journal of Computers and Security. Vol.24.No.7. October, pp.529-545. 2005.

[3] Jonatan Gomez & Dipankar Dasgupta,Evolving Fuzzy Classifier for Intrusion Detection,Proceedings of the 2002 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, 2001.

[4] Osareh Alireza & Shadgar Bita, “Intrusion Detection in Computer Networks based on Machine Learning Algorithms”. International Journal of Computer Science and Network Security, Vol.8.No.11. November, pp.15-23, .2008.

[5] Hamid Roomi Talkhaby, Reza Parsamehr, “Cloud Computing Authentication Using Biometric-Kerberos scheme based on Strong Diffi-Hellman-DSA Key Exchange”, 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)

[6] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” Journal of Network and Computer Applications, vol. 79, pp. 88– 115, 2017.

[7] J. S. Yang and H. K. Choi, “Ip based security architecture of virtual network in cloud computing system,” in 2012 8th International Wireless Communications and Mobile Computing Conference

(IWCMC), 2012, pp. 709–715.

[8] P. P. Ray, "A survey of iot cloud platforms," Future Computing and Informatics Journal, pp. –, 2017.

[9] J. Lee and D. R. Stinson, Deterministic Key Predistribution Schemes for Distributed Sensor Networks. Springer Berlin Heidelberg, 2005, pp. 294–307.

[10] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," IEEE Des. Test, vol. 24, no. 6, pp. 522–533, Nov. 2007.

[11] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 201, ISSN: 2278 – 1323

[12] L. Wang, G. Laszewski, M. Kunze and J. Tao, "Cloud computing: a perspective study", J New Generation Computing, 2010, pp 1-11.

[13] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[14] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing, "2009, http://www.wheresmyserver.co.nz/storage/ media/faq-files/clouddef- v15.pdf, Accessed April 2010.

[15] R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[16] Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay.

[17] J.H. Lee, M.W. Park, J.H. Eom, T.M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", In 13th International Conference on Advanced Communication Technology, pp.552-555, 2011.

[18] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291 (SP500- 291)," Gaithersburg, July 2011.

[19] D. M. Cappelli and R. F. Trzeciak, "Best practices for mitigating insider threat: Lessons learned from 250 cases," [Online]. July 2013, Available: http://www.cert.org/archive/pdf/RSA-CERTInsiderThreat.pdf.

[20] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider Attacks in Cloud Computing," Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, 2012, pp. 857–862.

[21] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, January 2013.

[22] J. C. Roberts II and W. Al-Hamdani, "Who Can You Trust in the Proc. Information Security Curriculum Development Conference, Kennesaw, 2011, pp. 15-19.

[23] M. K. Srinivasan and P. Rodrigues, "State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud," Proc. 2nd International Conference on Advances in Computing, Communications and Informatics," Mysore, 2012, pp. 470-476.

[24] S. Meena, E. Daniel and N. A. Vasanthi, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," Proc. International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, 2013, pp. 1076-1081.

[25] Computing," Energy Procedia, vol. 13, pp. 7902-7911, 2011. [16] U. Oktay, M. A. Aydin and O. K. Sahingoz, "Circular Chain VM Protection in AdjointVM", Proc. The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE2013), Konya, 2013, pp. 94-98.

[26] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94 (SP800-94)," Gaithersburg, February 2007.