ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Integrated Security with Public Cloud

Surya Verma[1] and Vimmi Pandey [2]

UG Scholar, Department of Computer Science and Engineering, Gyan Ganga College of Technology, Jabalpur[1]

Professor, Gyan Ganga College of Technology, Jabalpur[2]

Abstract: Cloud computing is being used in every applications of web technology including web applications, mobile communication and remote data access oriented applications. This is also threatening for the information of the users of these cloud computing. Most important of the threats in Cloud computing is security of the data of the users as it is being posted over the cloud and can be manipulated, misused by the other cloud users, cloud service providers or hackers. Various researchers have worked on cloud computing security and many algorithms have been developed. Still because of rapidly changing technologies, devices and applications demand continuous work in the field of security of data over cloud. Conventionally data security is applied using encryption/decryption key management, Intrusion Detection and Prevention systems for the networks. Applications of these techniques over the cloud makes it secured but in parallel ill minded persons are also developing tools and techniques to crack these security measures. This work is providing detailed discussions on possible security threats, solutions developed by the other researchers and an integrated security solution for the same. It will use cryptography techniques, trust management and application of Intrusion Detection Systems collectively for applying the security.

Keywords: Cloud Computing, Security, Intrusion Detection System, Encryption, Decryption, Authentication, Authorization, non-repudiation.

I. INTRODUCTION

As the amount of data being generated and transmitted over to the cloud increases, so too do research proposals to combat security issues with advanced cryptography. Often these proposals involve complex policy algorithms and new infrastructures, which work in theory, but would require high overhead in reality.

Dr. Mazhar Ali, however, may have found a simpler answer that offers both increased cloud security and affordable implementation. In his recently-published methodology, he suggests simply splitting encryption keys into two parts so that no single user has access to everything. Standard data sharing in the cloud involves symmetric encryption, which is the oldest and most popular technique using one key to both encrypt and decrypt files. However, this method presents major security concerns for two reasons: a) it's too easy for the key to fall into the wrong hands internally, and b) it's too difficult to frequently modify the key with personnel changes, so departing members can often continue to access sensitive information long after they're gone.

Rather than restructure the current cloud paradigm, Ali and his team decided to work within it to find a practical solution that could be deployed immediately. The key? Secure Data Sharing in Clouds, or SeDaSC, methodology.

The below image summarizes how SeDaSC works between a user, the cloud platform, and a trusted third-party cryptographic server (CS), which is responsible for key management, encryption, decryption, and access control.

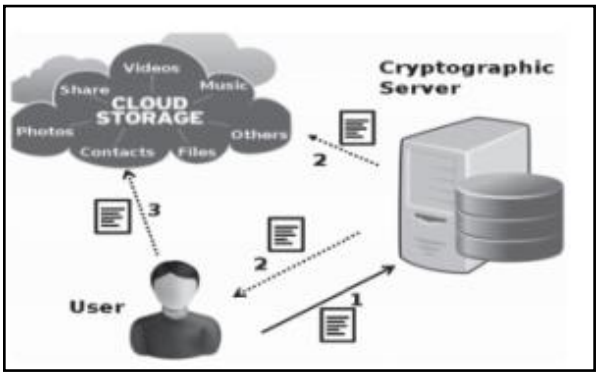

Figure 1: Cloud Security application using SeDaSC

SeDaSC adds an extra checkpoint to the standard process by making the encryption key a basic two-piece jigsaw puzzle that can be defined by the access control list (ACL). At the same time, SeDaSC doesn't require the high overhead of re-encryption or intense computations, so data access is still fast, and can work with mobile devices.

"In computer science and engineering, it's easy to get caught up in complicated concepts, and then feel inclined to build those out to become even more complicated," Ali said. "Sometimes you need to take a step back and determine what makes sense in our existing infrastructure. For us, a relatively simple solution just clicked. SeDaSC enables government and enterprise entities to more-securely manage their sensitive data today."

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

The team tested its methodology with Amazon Cloud services and its own CS, and found that it was the quickest secure data-sharing method when compared to other contemporary works. The only downside is that communication time would take a bit longer than usual because the user would have to request data via the CS. But even then, it's split-seconds.

SeDaSC has not yet been adopted by organizations, but according to Ali, it's gotten quite a bit of interest from other researchers since it was published, and the only thing standing in the way of deployment is a basic code in the CS to divide the key.

In recent years, cloud computing has rapidly emerged as a widely accepted paradigm in computing systems, in which an end-user can request some computing capabilities and services when he need it, and he can reach these resources across networks anytime, anywhere. Pew Research Institute published a research about "the future of cloud computing", and depicted that about % 71 of technology stakeholders and critics believe that by the year 2020, most people will work in Internet-based applications, which can also be run from smart phones [22]. Therefore, it can be seen that the future of cloud computing technology is bright and will be widely used in the World. While moving from traditional local computing paradigm to the cloud computing paradigm, new security and privacy challenges emerge because of the distributed nature of cloud computing. Some of these security vulnerabilities leave open doors, which stem from the existing computing models and some of them, inherent from cloud-based models. As a result, malicious users force these doors to attack the system, and they attack on end-users' private data; processing power, bandwidth or storage capacity of the cloud network. Cloud computing organizations have to provide a high quality service and protect the users' sensitive data. To prevent these attackers, firewall mechanism and/or Intrusion Detection System (IDS) are effective solutions to resist them. They can provide additional protection mechanisms on the cloud systems' distributed environments.IDS can identify suspicious activities by monitoring network traffic changes, configuration of the system, logs files, and actions of end-users. When such a suspicious event is detected, IDS sends an alert message to a person or monitoring console to trigger some actions for preventing these attacks. Cloud computing is an emerging paradigm that allows customers to obtain computing services and resources such as networks, servers, storage and applications. It provides services according to a pay-per-use business model [1]. Cloud computing has a high demand because it enables IT managers to provision services to users sooner and in a gainful way. Cloud computing technology has been facing some security issues. Cloud computing operational models, enabling technologies and its distributed nature, clouds are easy targets for intruders [2].

Many intrusion detection and knowledge security approaches for securing cloud are planned and are in applying [5, 6].

In an exceedingly recent analysis paper by, Rocha and Correia [19] presents however malicious insiders will steal confidential knowledge. Anup gosh and Chris Greamo [20] has presented however malware effects cloud computing setting. A multi-agent based mostly system for intrusion detection by Islam M.Hegazy et al [21] has delineated a framework for intrusion detection mistreatment agent based mostly technology. Hisham A.Kholidy et.al [22] has planned a framework for Intrusion Detection in cloud systems wherever IDS is deployed in the slightest degree the nodes together with info that ought to even be secured. Associate in Nursing autonomous agent primarily based intrusion detection system for cloud environments has planned agent based model with sensors by watching business flows client behaviour are often expected will confirm DoS attacks [23].For For this year's International Symposium on Space Terahertz Technology, the organizing committee has decided to request extended abstracts from potential presenters that can be published as part of the conference proceedings in place of final papers submitted after the conference. This will allow a much more timely publication of the conference proceedings, and should make it easier for preliminary work presented at the conference to be completed and submitted to refereed journals as full publications following the conference.

We present the identified existing intrusion attacks, existing intrusion detection and prevention techniques and drawbacks of existing IDPS solution for cloud intrusion attacks. We propose novel cloud service usage profile based intruder detection and prevention system to some of the cloud intrusion attacks. It detects and prevents intrusion based on their regular cloud service usage profiles. Usage profile may consist of many parameters like regular usage time, usage roles, usage privileges, usage logs and etc.

Section I is introduction of Cloud and the usage of the cloud. Section II discussion the major areas of the threats in Cloud with the specific threats in Cloud security. Section III discusses the work done by the other authors in the area. Section IV proposes some of the possible schemes for the security of the Cloud. Section V discusses the results and finally conclusion this research has been discussed.

II. 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

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

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 [4] 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 [8]. 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 [9, 10]

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 [11].
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 [12].
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 [13].
Data Modification, Forgery and Integrity: Un-trusted providers and system administrators can manipulate users' and consumers' data among to their own benefits [14, 15, and 16].

III.EXISTING SYSTEM

Users of cloud computing don't have presently acceptable tools for his or her verification of confidentiality, privacy policy, computing accuracy, and information integrity. To touch upon this downside, a brand new approach referred to as trustworthy Cloud Computing Infrastructure is projected galvanized by trustworthy Cloud Computing Platform. Through presenting a User trustworthy Entity (UTE) the projected approach is meant to form cloud computing infrastructures reliable so as to alter infrastructure service developers to supply a closed execution surroundings. One advantage of the projected UTE is that managers of Infrastructure as a Service (IaaS) systems have no privilege among UTE. So cloud computing managers cannot interfere in trustworthy organiser practicality. It's been assumed UTE ought to be unbroken by a 3rd agent with none incentives to interact with IaaS services and extremely trustworthy to make sure confidential execution of guest virtual machines. Additionally, UTE permits users to manifest IaaS server and confirm the safety of cloud service before start-up of virtual machine.
Cloud computing becomes a lot of and a lot of acquainted to individuals, and its application field becomes a lot of and a lot of wide. The way to build secure pc cloud computing environments becomes one amongst the recent analysis subjects. During this paper, from the definition of vaporization computing, introduced its development standing and anal sized the safety issues. Advance some trains of considered the safety, and eventually this paper believes that trustworthy cloud computing are a promising direction of the longer term cloud security researches.
Nowadays, cloud computing becomes quite popular and a lot of research is done on services it provides. Most of security challenges induced by this new architecture are not yet tackled. In this work, we propose new security architecture, based on a massively distributed network of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

security solutions, to address these challenges. Current solutions, like IDS or firewalls, were not formerly designed to detect attacks that draw profit from the cloud structure. Our solution Discus is based on a distributed architecture using both physical and virtual probes, along with former security solutions (IDS and firewalls). This paper describes Discus Script, a dedicated language that provides an easy way to configure the components of our solution. [1]

Cloud computing has enabled elastic and transparent access to distributed services, without investing in new infrastructures. In the last few years, Cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. Despite of all the hype surrounding the Cloud, enterprise customers are still reluctant to deploy their business in the Cloud. Security is one of the major issues which reduces the growth of Cloud computing and complications with data privacy and data protection continue to plague the market. In this paper, we propose a solution for Hybrid Cloud security, focusing on a Virtual Intrusion Detection System (V-IDS). We present a new architecture that considers the basic principles of the Cloud computing, virtualization and GMPLS Control Plane and applies them to the intrusion detection systems, in order to protect Cloud networks characterized by constantly changing of the underlying infrastructure and physical topology. Based on the defined architecture, we have implemented a prototype of Cloud based IDS that validates our thesis. The prototype is realized though the integration of two open-source technologies: OpenStack and DRAGON (Dynamic Resource Allocation via GMPLS Optical Networks). [2]

Cloud Computing emerge as new IT paradigm, which aims to provide applications delivered as services over the Internet and the hardware and systems software in the data centres that provide those services, by sharing resources to achieve coherence and economies of scale. However, one of the most important occupations of cloud computing today is to ensure the security of the infrastructure. This paper brings an introduction to the virtualization in a cloud environment. In the first place we will describe the principle of operation of a virtual network in the platform Xen, then we will discuss some possible attacks on these networks. In the end, we will introduce an analysis of some models of IDS applied to the cloud computing. [3]

Cloud computing is an enticing field nowadays due to its cost effective nature, easy accessibility, the pay per use service and shared resources. These shared resources, easy accessibility and shared storage of resources are responsible for putting the confidential information under a great deal of risk. Although the cloud is becoming gigantic day by day but its efficiency is being hampered considerably due to the threats in the cloud computing environment. The threats in the cloud computing environment not only account to external attacks which are launched with the intention of hampering work flow of the cloud provider but the internal attacks also which are being launched so that the efficiency and the reliability of the cloud is at stake. The firewalls monitor traffic between networks such that all the traffic must flow through it, but they are certainly not sufficient to shield the dynamic cloud computing environment from all attacks. They may be able to subvert external attacks to a certain extent but internal attacks do not even pass through the firewalls, therefore rendering them useless. Moreover, attackers exploit vulnerabilities in the virtual machines in order to set up large scale attacks like Ddos. They compromise these VM's into zombies and the detection of these VM's is very difficult because cloud users install all types of applications onto their VM's some of which may be malicious. Thus, the cloud needs stronger security for handling all the intrusions of every scale. An intrusion detection system is presented in the paper which detects the intrusions launched on the VM's which act an avenue for deploying large scale attacks, therefore, minimising the loss. The IDS presented in the paper is a network IDS and provides security from the IaaS based attacks. [4]

Nowadays, Cloud Computing is the first choice of every IT organization because of its scalable and flexible nature. However, the security and privacy is a major concern in its success because of its open and distributed architecture that is open for intruders. Intrusion Detection System (IDS) is the most commonly used mechanism to detect various attacks on cloud. This paper shares an overview of different intrusions in cloud. Then, we analyze some existing cloud based intrusion detection systems with respect to their various types, positioning, detection time, detection techniques, data source and attacks. The analysis also provides limitations of each technique to determine whether they fulfill the security needs of cloud computing environment or not. We highlight the deployment of IDS that uses multiple detection methods to manage with security challenges in cloud. [5]

Computing in cloud has come out as a growing trend that has eliminated the burden of hardware and software infrastructure by facilitating virtual machines via internet. In spite of the indispensable advantages, cloud computing also brings critical challenges that cannot be avoided from consumer side if the security of the data is concerned. In this paper, we analyze the various security aspects that are vulnerable to the cloud computing and needed to be resolved. This will help to upgrade promising benefits of cloud computing so that consumers cannot have a second thought regarding its adoption. [6]

Cloud computing has emerged as an increasingly popular means of delivering IT-enabled business services and a potential technology resource choice for many private and government organizations in today's rapidly changing computing environment. Consequently, as cloud computing technology, functionality and usability expands unique security vulnerabilities and treats requiring timely attention arise continuously. The primary challenge being

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

providing continuous service availability. This paper will address cloud security vulnerability issues, the threats propagated by a distributed denial of service (DDOS) attack on cloud computing infrastructure and also discuss the means and techniques that could detect and prevent the attacks. [7] A survey on security problems in commission delivery models of cloud computing Cloud computing could be a thanks to increase the capability or add capabilities dynamically while not investment in new infrastructure, coaching new personnel, or licensing new software system. It extends data Technology's (IT) existing capabilities. Within the previous few years, cloud computing has adult from being a promising business conception to at least one of the quick growing segments of the IT trade. However as a lot of and a lot of data on people and firms area unit placed within the cloud, considerations area unit starting to grow concerning simply however safe A surroundings it's. Despite of all the promotional material encompassing the cloud, enterprise customers area unit still reluctant to deploy their business within the cloud. Security is one amongst the foremost problems that reduces the expansion of cloud computing and complications with information privacy and information protection still plague the market. The appearance of a complicated model shouldn't talk terms with the specified functionalities and capabilities gift within the current model. a brand new model targeting at rising options of AN existing model should not risk or threaten alternative necessary options of the present model. The design of cloud poses such a threat to the safety of the present technologies once deployed in very cloud surroundings. Cloud service users have to be compelled to be argus-eyed in understanding the risks of information breaches during these new surroundings. During this paper, a survey of the various security risks that cause a threat to the cloud is bestowed. This paper could be a survey a lot of specific to the various security problems that has emanated because of the character of the service delivery models of a cloud automatic data processing system. The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software system delivery and development models. protrusive as AN biological process step, following the transition from mainframe computers to client/server preparation models, cloud computing encompasses parts from grid computing, utility computing and involuntary computing, into AN innovative preparation design. This speedy transition towards the clouds has fuelled considerations on a important issue for the success of knowledge systems, communication and knowledge security. From a security perspective, variety of unchartered risks and challenges are introduced from this relocation to the clouds, deteriorating a lot of the effectiveness of ancient protection mechanisms.

As a result the aim of this paper is twofold; first off to gauge cloud security by characteristic distinctive security needs and second to aim to gift a viable resolution that eliminates these potential threats. This paper proposes introducing a trustworthy Third Party, tasked with reassuring specific security characteristics among cloud surroundings. The projected resolution calls upon cryptography, specifically Public Key Infrastructure operational collectively with SSO and LDAP, to make sure the authentication, integrity and confidentiality of concerned information and communications. The answer, presents a horizontal level of service, accessible to any or all involved entities, which realizes a security mesh, among that essential trust is maintained.

IV. PROPOSED SCHEME

An integrated solution of the security threats in cloud is a possible scheme which is going to be helpful for all the different types of users of the cloud. It will be a combination of the

Phase I

Log collection module: The network packets are collected from network, Includes: network source port, destination port, the length of the connection over time, the use of network bandwidth. Collect log data from Super Manager hypervisor.

Phase II

Log data storage module: The collected log data are matched with the rule base. If the behaviour is abnormal, alarms are generated and transmitted to security management centre for response.

Phase III

Analysis module: The logs are collected and saved into the log table, then passed to analysis module based on rough set to process, new decision-making rules are generated.

All phases work accordingly to given architecture presented below.

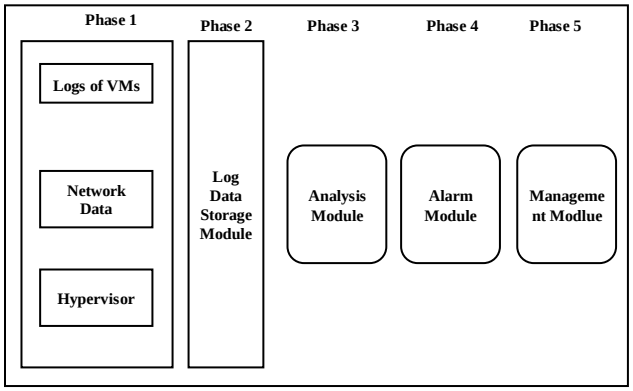

Figure 1: Proposed Computing Intrusion Detection model

Phase IV

Alarming module: The collected logs are matched with the decision-making rules in the rule database.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

If it is abnormal behaviour then system will generate alarms.

Phase V

Cloud computing management module: Abnormal alarms are transmitted to cloud computing security management centre which irresponsible for real-time response.

V. PROPOSED METHODOLOGY

The proposed implementation shall be done using following methodology:

Step 1: Authentication System, Users will require to undergo an initial authentication system, which will verify the existence of the users in the system by taking his/her authentication details which will include a key and a password. The key will be verified on two places that is first on a trust server and secondly on cloud. The key and password inputted shall be encrypted and sent to the cloud; cloud verifies the same by sending the encrypted details to the trust server. Trust server will keep the client details and will inform to the cloud about the verified key and will also send a substitute for session management of the client.

Step 2: Authorisation,

1) From Client to Cloud: once the authentication has been completed, the user can invoke data transfer module for which he will have to first get checked with authorities. For authorisation, client will move to data transfer page i.e. from client to cloud. As this page shall be opened, cloud will send the session key to the trust server, which will send it in turn to KDC (Knowledge Data Centre). KDC will verify the authorization of client and will inform about it to the trust server. Trust server will send another key to cloud stating whether the user is having proper authorisation for data transfer or not.

2) From Cloud to Client: a must have proper authorization to retrieve data. Similar process as in first point shall be executed to retrieve the authorization before providing the data to the client.

Step 3: Intrusion Detection: On cloud / trust server a system will be developed to test about the usage being applied by the client from a particular account or for a particular data. If the frequency of access is more within a time interval then intruder alert is generated which is prevents the request of the client from executing.

VI. PROPOSED ALGORITHM

The complete system shall be implemented using the following algorithms:

Algorithm Authenticate (eusername, epassword) {

```
Cloud Transfers eusername, epassword to trust server
Username := decrypt(eusername);
Password := decrypt(epassword);
Result := verifyUsernamePasswordFromDb();
If(Result = Ok) {
   Key:=GenerateKey(Username, Password);
   Return Key;
}
Else {
   Error := “Invalid Username/Password”;
   Return Error;
}
}
```

Algorithm Authorize (ekey) {

```
Cloud Transfers ekey to trust server
Key := decrypt(ekey);
Result := sendKeyToKDC(Key);
If(Result = Ok) {
   AKey:=GenerateAuthorizationKey(Key);
   Return Key;
}
Else {
   Error := “Unauthorised User”;
   Return Error;
}
}
```

VII. CONCLUSIONS

Security of the data of the users of the Cloud is a mandatory requirement and the factors involved in security threats are too many. The focus of this research work is providing users a common and integrated security environment and helping to everyone involved in cloud operations including cloud users and service providers. Since the data being generated for cloud web apps is too much therefore efficient analysis of Data Integrity issues & its solution over the cloud environment by using proposed System shall be an outcome of this research.

This work shall further be providing a proposition of a novel & efficient approach over the cloud environment that will eliminate all potential threats related to cloud security.

ACKNOWLEDGMENT

I am Thankful to **Mrs Vimmi Pandey,** M.Tech, for providing proper guidance and provocation for completing my work and writing this paper. Her help and guidance is key for my forth coming endeavours to take this research.

REFERENCES

[1] Riquet, D.; Grimaud, G.; Hauspie, M., "Discus: A massively distributed IDS architecture using a DSL-based configuration," in Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on , vol.2, no., pp.1193-1197, 26-28 April 2014 doi: 10.1109/InfoSEEE.2014.6947859

[2] Donadio, P.; Fioccola, G.B.; Canonico, R.; Ventre, G., "Network security for Hybrid Cloud," in Euro Med Telco Conference

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

(EMTC), 2014 , vol., no., pp.1-6, 12-15 Nov. 2014 doi: 10.1109/EMTC.2014.6996640

[3] Bousselham, A.; Sadiki, T., "Security of virtual networks in cloud computing for education," in Web and Open Access to Learning (ICWOAL), 2014 International Conference on , vol., no., pp.1-5, 25-27 Nov. 2014 doi: 10.1109/ICWOAL.2014.7009218 [3]

[4] Maqsood, R.; Shahabuddin, N.; Upadhyay, D., "A Scheme for Detecting Intrusions and Minimising Data Loss in Virtual Networks," in Computational Intelligence and Communication Networks (CICN), 2014 International Conference on , vol., no., pp.738-743, 14-16 Nov. 2014 doi: 10.1109/CICN.2014.160

[5] Kene, S.G.; Theng, D.P., "A review on intrusion detection techniques for cloud computing and security challenges," in Electronics and Communication Systems (ICECS), 2015 2nd International Conference on , vol., no., pp.227-232, 26-27 Feb. 2015 doi: 10.1109/ECS.2015.7124898

[6] Kajal, N.; Ikram, N.; Prachi, "Security threats in cloud computing," in Computing, Communication & Automation (ICCCA), 2015 International Conference on , vol., no., pp.691-694, 15-16 May 2015 doi: 10.1109/CCAA.2015.7148463

[7] Goel, R.; Garuba, M.; Grima, A., "Cloud Computing Vulnerability: DDoS as Its Main Security Threat, and Analysis of IDS as a Solution Model," in Information Technology: New Generations (ITNG), 2014 11th International Conference on , vol., no., pp.307-312, 7-9 April 2014 doi: 10.1109/ITNG.2014.77

[8] C. B. Westphall and F. R. Lamin. SLA Perspective in Security Management for Cloud Computing. In Proc. of the Int. Conf. on Networking and Services (ICNS), 2010. Pp. 212-217.

[9] Hisham A. Kholidy, Fabrizio Baiardi CIDS: A framework for Intrusion Detection in Cloud Systems, 2012 Ninth International Conference on Information Technology- New Generations, 978-0-7695-4654-4/12 © 2012,pp 379-385.

[10] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology(NIST), Special Publication 800-94, Feb. 2007.

[11] 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.

[12] H. Jin, G. Xiang, D. Zou et al., "A VMM-based intrusion prevention system in cloud computing environment," The Journal of Supercomputing, pp. 1–19, 2011.

[13] T. Udaya, V. Vijay, and A. Naveen, "Intrusion detection techniques for infrastructure as a service cloud," in Proceedings of the 9th IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE Computer Society, pp. 744–751, Sydney, Australia, 2011.

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

[15] 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.

[16] [10] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

[23] G. Tyler, "Information Assurance Tools Report Intrusion Detection Systems," Information Assurance Technology Analysis Center (IATAC), September 2009.

[24] F.Rocha,M. Correia,2011,Lucy in the sky without diamonds: Stealing confidential data in the cloud.

[25] Anup ghosh, Chrish greamo, page 79-82, 2011, "Sandboxing and Virtualization", Security and privacy,IEEE.

[26] Islam M. Hegazy, Taha Al-Arif, Zaki.,T. Fayed, and Hossam M. Faheem ,Oct-Nov 2003,"Multi-agent based system for intrusion Detection" ,Conference Proceedings of ISDA03, IEEE.

[27] Hisham A. Kholidy, Fabrizio Baiardi, 2012 CIDS: "A Framework for Intrusion and Detection in cloud Systems", 9th International Conference on Inform- ation Technology- New Generations,IEEE.

[28] Frank Doelitzscher∗ , Christoph Reich∗ , MartinKnahl and Nathan Clarke, p197-204, 2011,"An autonomous agent based incident detection system for cloud environments", 3rd IEEE International Conference.

[29] Kawser Wazed Nafi , Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[30] R Rangadurai Karthick,Vipul P. Hattiwale, Balaraman Ravindran "Adaptive Network Intrusion Detection System using a Hybrid Approach" 978-1-4673-0298-2/12/$31.00 c 2012 IEEE.

[31] Siva S. Sivatha Sindhu , S. Geetha , A. Kannan "Decision tree based light weight intrusion detection using a wrapper approach" Expert Systems with Applications 39 (2012) journal homepsage: www.elsevier.com/locate/eswa.

[32] Sung-Bae Cho and Hyuk-Jang Park "Efficient anomaly detection by modeling privilege flows using hidden Markov model" Computers & Security Vol 22, No 1, pp 45-55, 2003

[33] Dinesha H Aand Dr. V.K Agrawal "MULTI-DIMENSIONAL PASSWORD GENERATION TECHNIQUE FOR ACCESSING CLOUD SERVICES" International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.3, June 2012.

[34] Md Kausar Alam, Sharmila Banu K "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds "International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153 www.ijsrp.org .

[35] Mohit Marwaha, Rajeev Bedi "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing"IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 www.IJCSI.org.

[36] Richa Sondhiya, Maneesh Shreevastav, Mahendra Mishra "To Improve Security in Cloud Computing with Intrusion detection system using Neural Network" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[37] Ms.Asha.D and R.Chitra "Securing cloud from ddos attacks using intrusion detection system in virtual machine" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 - 8791

[38] Kashif Munir and Sellapan Palaniappan "Security Threats/Attacks Present in Cloud Environment".

[39] Flavio Lombardi, Roberto Di Pietro "Secure virtualization for cloud computing" Journal of Network and Computer Applications 34 (2011) 1113–1122.