Instruction detection over over Cloud: a Survey

Pooja Jayant[1], Nitesh Gupta [2], Umesh Lilhore [3]

[1,2,3]*Computer Science & Engineering, NRI Institute of Information Science & Technology, Bhopal India*

---***---

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 paper discusses cryptography techniques, trust management and application of Intrusion Detection Systems collectively for applying the security.*

Key Words: Cloud Computing, Security, Intrusion Detection System, Encryption, Decryption, Authentication, Authorization, non-repudiation

1. INTRODUCTION

Internet of things is no more a buzzword now. It is a connected network of people, things, process, and data or basically everything. IoT is a concept of connecting anything to the Internet from our daily used items like bed alarm, cell phones, watches, dishwasher etc. It composed of various sensors, actuators, and networking devices etc. that enables the things to acquire the data, transform it into information and then knowledge and wisdom, take decisions based on them and manipulate the environment. With the evolution of IPv6, there can be 2128 unique addresses possible. According to a survey of Cisco, there would be more than 30 billion connected devices in 2020. More the data, the better understanding we can obtain. But handling the vast amount of data that generated from this huge number of things is very challenging for the researchers. The main characteristics of this IoT data can be stated as-Variety, from heterogeneous sources and data formats, from text to images, scripts, videos etc, Volume or scale of data from the huge quantity of connected sensors and their intercommunications, which create Velocity or dynamic factor in data. Also, according to some studies, only 30% of the data collected by the sensors is valuable or correct. So, this low-level data but in extent amount first need to be stored, then processed and accessed from multiple dimensions for efficient analysis. Acquisition, integration from various sources, distributed storage especially in cloud platforms, processing, analyzing and using the insights of this huge data is the giant problem and novel area of research for the data scientists. Distributed environment is needed to process such data. Also, as most of the things of IoT are small and inexpensive end user devices like smartphones, tablets, wearable devices etc., there are the issues of the limited power supply, low storage, processing capabilities etc. There comes the need of integration of Internet of things with Cloud platform. Applications can be backed by the cloud services. Cloud computing is a service-based architecture with a shared and configurable pool of resources. Virtualization is the key technique. Services like networking, computation, storage are provided to the user on an on-demand basis. It saves expenditure on hardware and other resources and let the organization focus on their core business. With the platform of cloud, mining and analysis of huge data of ubiquitous sensors of IoT can be advanced with virtually unlimited resources and capabilities of the cloud.

From past few years, technology industry has been steadily moving away from local storage to remote, server-based storage and processing—known as *the cloud*. And this kind of storage technology has made it possible to access personal data from anywhere and at anytime. For example: Focusing on the entertainment industry one can observe that music and movies where previously majorly stored in local media, but now they're streamed from servers because one gets the same benefits of watching movies and listening to music from anywhere, at anytime and with sharing capability from and because of cloud storage and processing service.

These services provide easy access to all your important and private data—Word documents, PDFs, spreadsheets, photos, any other digital assets. For every individual and organization today, cloud is an efficient technology to keep their data on[1]. And that's the reason many organizations collecting information, from customers, sensors, or any other possible and required sources of data, for use or providing some service prefer cloud storage service. This eventually accommodates huge amount of data (of both types: important and not so important) about a lot of people, organizations and things on the cloud.

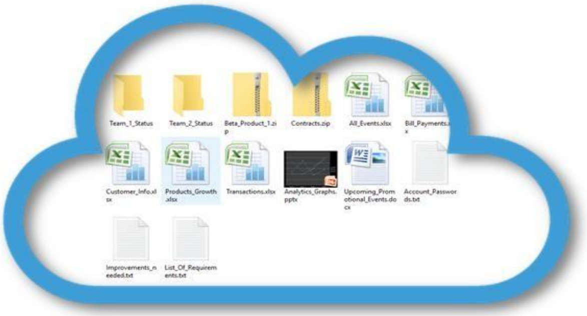

Fig. 1.1. Abstract explanation of Cloud concept

This service along with its numerous benefits is subject to many threats. And possibly the most dangerous one is Data Theft [2]. Data theft attacks can harm both individuals as well as organizations, whether they'd be the users of cloud or cloud service providers.

These data thieves, if insiders from the organization cause even more harm to the organization. The reason why it is easy for insiders to perform data theft attacks is because they are given the right to access data kept on cloud by the company itself because the insiders require that data for their work. And thereby stealing a customer's admin passwords is easier for a malicious insider than an outsider.

Insider data theft would lead to both internal integrity degradation of the company as well as would put at risk Company's external reputation. It will probably also lead to losing customer's trust in the organization or company because of their private data getting leaked [3].

2. CLOUD OF THINGS

The integration of cloud computing and IoT can facilitate the sharing of resources more efficiently. Resources here are the services of clouds, which may be in form of software, computing or infrastructure. Cloud computing can provide a virtual infrastructure for all the needs like storage, analytical tools, monitoring, visualization etc. This integration is called as Cloud of Things. The huge sensing data can be stored in clouds and can be used intelligently for smart monitoring with various algorithms of data mining, machine learning methods, and techniques of artificial intelligence. Automated decision-making and various novel applications such as smart healthcare, smart cities, transport systems and grids can be achieved in this way. The services of the clouds named as Software as a Service, Infrastructure as a Service and Platform as a Service are drawn-out to additional services like Data as a Service, Sensor Event as a Service, Ethernet as a Service, Sensing and Actuation as a Service, Identity and Policy Management as a Service etc. Although the integration gives us major development goals for various smart applications, yet the cloud platform cannot be used directly for complex models like MapReduce etc. The framework should provide support for reading, processing, and generating output from streams. During the integration, Quality of Service, security of data, privacy, reliability and other critical factors are concerned. Smart gateways are required to perform the task of preprocessing. What type of data and how much of it is required to transfer to the clouds are critical issues. There are various other factors related to the integration which can be summarized as follows-

- **Protocol support -** For different things, different protocols are there. IoT uses Wifi, ZigBee, 6LoWPAN etc. Some machines connect to a controller using protocols other than IP. Cloud uses IP. Protocols support and adaptation is necessary between the two paradigms.
- **Data Communication -** Data communication management between clouds and IoT is indispensible. It is not necessary to transfer all the data from the sources to the clouds.
- **Energy Efficiency -** Data communication between sensors, actuators and cloud consumes much power. An efficient power supply is required for a large number of things. A flexible and consistent management for energy consumption is required.
- **Resource allocation-** when there are too many sensors, there would be too many requests for the resources. It's difficult when different IoT demands same type of resources. Cloud manager should take care of this allocation based on type, purpose, and frequency of demand for sensors.
- **Service Discovery-** In IoT, anything can leave or add into the network anytime. A uniform way is required to discover and manage the status of the services.
- **Data processing and Mining-**Acquisition, Storage, Management, Optimization
- **Sharing of sensing services and cloud applications-** Services of clouds are extended with IoT services like sensing as a service. Many other kinds of services can be identified.
- **Low Latency and awareness of location-** IoT requires speedy responses which can advances the output and thus improves the levels of services and safety. Faster response is critical for industries like manufacturing, thermals, oil & gas, public sector etc, which prevents the cascading failure.
- **Heterogeneity-** Billions of things are composed of thousand of types. And their data formats are also different. The factor of heterogeneity needs to be managed.

- **Security & Privacy-** Sensitive data should be encrypted while transferring to and fro from the clouds
- **Quality of Service-** As the volume of data increase, type and unpredictability also increase. Service quality should be maintained depending on type and urgency of data.

3. LITERATURE REVIEW

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 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, minimizing 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 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.

Rocha and Correia contour passwords may be stolen very easily by a malicious insider of the Cloud service provider [4]. Just by stealing a customer's password and private key, the malicious insiders get to access all the customer data, also the customer being totally unaware of this unauthorized access detection.

Cloud computing security mechanisms have focused on preventing unauthorized and illegitimate access to the customer's web account and data in it. They have made an attempt to do this by developing sophisticated access control and encryption mechanisms. However these mechanisms are unable to prevent data compromise. It is proved that fully homomorphic encryption, which is often considered to be the solution to such type of threats, is not a full proof security mechanism for data protection when used single- handedly [5].

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.

4. 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

4.1 Characteristics Of Cloud Computing

a. Broad network access
b. On-demand self-service
c. Location Independence Customer
d. Resource pooling

4.2 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.

a. Data location
b. Regulatory compliance
c. Recovery
d. Privileged user access Risks In Cloud Computing.

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

a. Security of data in transit.
b. Security of data at rest.
c. Cloud legal and regulatory issues.
d. Robust separation between data belonging to different customers.
e. Authentication of users/applications/processes.
f. Indecent response.

5. 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].

6. Conclusion

A huge number of internet users are employing cloud computing for data storage. And as a result, proper security in potentially vulnerable areas of cloud storage technology has become a major point of concern for the users contracting with a cloud service provider. Strong and robust techniques for securing data on the cloud are thereby a compulsive need to the cloud service providers, to provide reliable service and cloud storage service users, to rely on the service providers. For securing data on the cloud, encryption and sophisticated user access are major techniques used. But these techniques corroborate to be weak in preventing data theft attacks when the data thief is a malevolent insider to the cloud service provider.

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 (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.

[4] 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

[5] 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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] [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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

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

[22] F.Rocha,M. Correia,2011,Lucy in the sky without diamonds: Stealing confidential data in the cloud. Anup ghosh, Chrish greamo, page 79-82, 2011, "Sandboxing and Virtualization", Security and privacy, IEEE.

[23] 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. 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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 homepage: www.elsevier.com/locate/eswa.

[28] 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

[29] 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 .

[30] 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.

[31] 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.

BIOGRAPHY

Pooja Jayant Mtech From Computer Science & Engineering In Nri Institute Of Information Science & Technology Bhopal. B.E From Computer Science & Engineering From SSSIST Sehore.