ISSN 2277-3061

ENHANCED SECURITY MECHANISM IN CLOUD COMPUTING: A REVIEW

Gagandeep Kaur [(1)], Dr. Mohita Garg [(2)], Mrs. Navjot Jyoti [(3)]
[(1)] Research Scholar, Department of Computer Science Engineering, NWIET, Moga
gagankhera101@yahoo.com
[(2)] Associate Professor, Department of Computer Science Engineering, NWIET, Moga
mohita_cse@northwest.ac.in
[(3)] Assistant Professor, Department of Computer Science Engineering, NWIET, Moga
navjot_cse@northwest.ac.in

ABSTRACT

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices. Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. We will be implementing cloud security aspects for data mining by implementing cloud system. After implementing cloud infrastructure for data mining for cloud system we shall be evaluating security measure for data mining in cloud. We will be fixing threats in data mining to Personal/private data in cloud systems.

Keywords

Cloud Computing, Cloud Security, Confidentiality, Security Issues, Zones, Grouping.

ISSN 2277-3061

INTRODUCTION

It is the model for convenient on-demand network access, with minimum management efforts for easy and fast network access to resources that are ready to use. It is an upcoming paradigm that offers tremendous advantages in economic aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. Popularity of cloud computing is increasing day by day in distributed computing environment. There is a growing trend of using cloud environments for storage and data processing needs. To use the full potential of cloud computing, data is transferred, processed, retrieved and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. Their main concerns are the confidentiality, integrity, security and methods of mining the data from the cloud. The Greek myths tell of creatures plucked from the surface of the Earth and enshrined as constellations in the night sky. Something similar is happening today in the world of computing. Data and programs are being swept up from desktop PCs and corporate server rooms and installed in “the compute cloud”. In general, there is a shift in the geography of computation. Computing can be described as any activity of using and/or developing computer hardware and software. It includes everything that sits in the bottom layer, i.e. everything from raw compute power to storage capabilities. Cloud computing [1] ties together all these entities and delivers them as a single integrated entity under its own sophisticated management.

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices.

CLOUD TYPES

Depending on infrastructure ownership, there are four deployment models of cloud computing [6].

1) **Public Cloud**: - Public cloud [4] allows users to access the cloud publicly. It is access by interfaces using internet browsers. Users pay only for that time duration in which they use the service, i.e., pay-per-use.

2) **Private Cloud**: - A private clouds [5] operation is with in an organization’s internal enterprise data center. The main advantage here is that it is very easier to manage security in public cloud. Example of private cloud in our daily life is intranet.

3) **Community Cloud**:-When cloud infrastructure construct by many organizations jointly, such cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community.

4) **Hybrid Cloud**: - It is a combination of public cloud [7] and private cloud. It provide more secure way to control all data and applications. It allows the party to access information over the internet. It allows the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for some computing resources.

SECURITY CONCERNS IN CLOUD COMPUTING

In this section we first introduce some major security concern-

• **Network Availability** The value of cloud computing [2] can only be realized when our network connectivity and bandwidth meet our minimum needs: The cloud must be available whenever we need it. If it is not, then the consequences are no different than a denial-of-service situation.

• **Cloud Provider Viability** Since cloud providers are relatively new to the business, there are questions about provider viability and commitment[9]. This concern deepens when a provider requires tenants to use proprietary interfaces, thus leading to tenant lock-in.

• **Disaster Recovery and Business Continuity** Tenants and users require confidence that their operations and services will continue if the cloud provider’s production environment is subject to a disaster.

• **Security Incidents** Tenants and users[3] need to be appropriately informed by the provider when an incident occurs. Tenants or users may require provider support to respond to audit or assessment findings. Also, a provider may not offer sufficient support to tenants or users for resolving investigations.

• **Transparency** When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider’s security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.

• **Loss of Physical Control** Since tenants and users lose physical control over their data and applications, these results in a range of concerns:

(a) Privacy and Data With public or community clouds, data may not remain in the same system, raising multiple legal concerns.

(b) Control over Data User or organization data may be comingled in various ways with data belonging to others.

(c) A tenant administrator has limited control scope and accountability within a Public infrastructure-as-a-service (IaaS) implementation[8], and even less with a platform-as-a-service (Paas) one. Tenants need confidence that the provider will

offer appropriate control, while recognizing that tenants will simply need to adapt their expectations for how much control is reasonable within these models.

(d) New Risks, New Vulnerabilities There is some concern that cloud computing brings new classes of risks and vulnerabilities. Although we can postulate various hypothetical new risks[10], actual exploits will largely be a function of a provider's implementation. Although all software, hardware, and networking equipment are subject to unearthing of new vulnerabilities, by applying layered security and well-conceived operational processes, a cloud may be protected from common types of attack even if some of its components are inherently vulnerable.

RELATED WORK

Alawode A. olaide [11] has proposed the concept of securityin the cloud. This paper discusses effort directed to which degree this skepticism is justified, by proposing to model Cloud Computing Confidentiality Archetype and Data Mining 3CADM. The 3CADM [10] is a step-by-step framework that creates mapping from data sensitivity onto the most suitable cloud computing architecture and process very large datasets over commodity clusters with the use of right programming model. To achieve this, the 3CADM determines the security mechanisms required for each data sensitivity level, which of these security controls may not be supported in certain computing environments, which solutions can be used to cope with the identified security limitations of cloud Computing.

Himeldev, Tanmoysen [12] has proposed the concept of privacy of the cloud data from data mining and attacks on the cloud data. We first identify the data mining based privacy risks on cloud data and propose a distributed architecture to eliminate the risks. Cloud data distributor is an entity that receives data from single client, where data is partitioned into multiple parts. These parts are distributed among several cloud providing companies.

Kangchan Lee [13] specifies Cloud computing is a model for enabli ng service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable comput ing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing enables cloud services. The security architecture and functions highly depend on the reference architecture.

Neha Tirthani [14] has contemplated a design for cloud architecture which ensures secured movement of data at client and server end. We have used the non breakability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. The proposed encryption mechanism uses the combination of linear and elliptical cryptography methods. It has three security checkpoints: authentication, key generation and encryption of data.

Amar Gondaliya [15] identifies security concerns arising in cloud computing environments and outlines methods to maintain compliance integrity and preserve security protection as virtual resources move from on-premise to public cloud environments. Many organizations that are providing security software that provides security control for cloud computing, but this paper provides the checklist of key questions for enterprise and service provider for cloud computing deployment.

Anthony Bisong [16] discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management.

R. Kalaichelvi Chandrahasan [17] specifies Cloud computing is a promising computing standard where computing resources in large data center are made available as services over Internet. Cloud computing has become prominent IT by offering the businessenvironment data storage capacity. This new profitable paradigm for computing is an attractive, massive, largescale investment that includes any subscription-based or pay-per-use service over the Internet. It is on-demand access to virtualized IT services and products.

Vahid Ashktorab [18] has cast light over the major security threats of cloud computing systems, while introducing the most suitable countermeasures for them. He also cited the aspect to be focused on when talking about cloud security. He has categorized these threats according to different viewpoints, providing a useful and little-known list of threats. After that some effective countermeasures are listed and explained.

MANDEEP KAUR [19] specifies Cloud computing is the internet based development and used in computer technology. The prevalent problemassociated with cloud computing is data privacy,security, anonymity and reliability etc. But the most important between them is security and how cloudprovider assures it. In this research paper, the proposedwork plan is to eliminate the concerns regarding dataprivacy using encryption algorithms to enhance thesecurity in cloud as per different perspective of cloudcustomers.

Mr.Tejas P.Bhatt [20] concern is to provide the security to end user to protect files or datafrom unauthorized user. Difference is that the research isdone in cloud, but security related issue can't be resolved yet.Security is the main intention of any technology throughwhich unauthorized intruder can't access your file or data incloud. Thus, we can give maximum effort to avoid the issuesof security occurs. We have designed one proposed designand architecture that can help to encrypt the file and decrypt it. In this research paper, we have used the AES Algorithm for the encryption.

Eng. Anwar J. Alzaid and Eng. Jassim M. Albazzaz [21] has proposed the concept of cloud computing in detail. Cloud computing is a relatively new term, it refers to a new way of processing and storing information this new style of processing promises to offer a huge amount of computing power to its users without requiring them to invest in expensive hardware.

A. Raja Rajeswari and R.Sakkaravarthi [22] has proposed the concept of data based privacy attacks in the cloud. As an alternative of maintaining personal data on the own hard drive or updating important applications for user needs, user can use a service over the network, to a different location, to store user information and / or use its applications. This also provides flexibility so it is very useful in a new generation of services and products. One of the main security[6] problems in cloud is data mining based privacy attacks that involve analyzing data over a long period to extract valuable information. It gives the outside attackers and providers having unconstitutional access to the cloud and a prospect of analyze the client information over an extensive period of time to extract the sensitive information that causes privacy violation of clients.

Cloud computing[4] involves distributed computing over a network, where a program or application may run on many connected computers at the same time. The cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data.

OBJECTIVES

Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. Malicious activity monitoring is a tough task in cloud system as logging data might be spread over multiple hosts and data centres. Restricting user to his own virtual partition only will not allow logs to be dispersed allowing access to logs for monitoring easily. User access is another major concern in restricting user access is a major challenge in cloud based storage system. Use of virtual partition and enhanced user access control in cloud system will allow us to improve data security. Enhanced Cloud system will be compared with existing secure cloud systems. We will compare enhanced system against security, performance & ease of use.

By distributing data on different clouds it introduces performance overhead when client needs to access all data frequently, e.g. client needs to perform a global data analysis on all data. The analysis may have to access data from multiple locations, with a degraded performance. By simply using in single cloud provider can having the following main issues: Less Security. Loss of data; No privacy; Cost of maintenance is high.

To enhance the security in cloud systems by creating user access policies:

• We will be enhancing the security by using single cloud provider and dividing single cloud into different zones thereby saving a cost of the client and also enhancing the security.

• We will segregate data by creating virtual partitions of data for saving and allowing user to access data in his partitions only. Each user will have the rights according to the role of the client i.e. role based access policies.

• Use of virtual partitions and enhanced user access control in cloud system will improve data privacy and thereby fixing the threats in data mining to personal / private data in the cloud systems.

• Cloud is divided into multiple zones.

• The zones chosen by the user are grouped together and the data of the user is stored inside the grouped zone.

• User will create his/her own account at the cloud Provider.

• Cloud Provider will assign the different privileges to the user depending upon the role of the user.

• Different access policies for different zones will be implemented over here.

• If the user has been assigned a role as a Read, then he/she can only read the data from the server.

• If the policy allows writing the data, then only user can write the data into the server.

• If the company tries to perform the mining at the user's data, then proper results will not be available.

We will be using the CloudSim as a simulator for implementing the proposed methodology. Cloud service providers charge users depending upon the space or service provided. In R&D [16], it is not always possible to have the actual cloud infrastructure for performing experiments. For any research scholar, academician or scientist, it is not feasible to hire cloud services every time and then execute their algorithms or implementations. For the purpose of research, development and testing, open source libraries are available, which give the feel of cloud services. Nowadays, in the research market, cloud simulators are widely used by research scholars and practitioners, without the need to pay any amount to a cloud service provider.

CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and

service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of thei r competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

REFERENCES

[1] Bhagyashree Ambulkar and Vaishali Borkar,"Data Security in Cloud Computing", MPGI National Multi Conference 2012 (MPGINMC-2012), 7-8 April 2012.

[2] Peter Mell, and Timothy Grance,"The NIST Definition of Cloud Computing", the National Institute of Standards and Technology, USA, 2011.

[3] ORACLE, "Cloud Security Techniques and Algorithms"

[4] M.Kantardzic, "Data Mining: Concepts, Models, Methods and Algorithms", John Wiley & Sons Inc., 2002.

[5] "Introduction to Cloud Computing Architecture", Sun Microsystems, 2009.

[6] "Top 10 Algorithms in Data Security", Springer-Verlag London Ltd., 2007.

[7] Jianzong Wang,Zhuo Liu, Peng Wang,"Data Mining of Mass Storage Based on Cloud Computing".

[8] M. Bramer. Principles of Data Security. Springer, 2007.

[9] M. Brantner, D. Florescu, D. A. Graf, D. Kossmann, and T. Kraska. Building a database on s3. In J. T.-L. Wang, editor, ACM, pages 251–264, 2008.

[10] S. H. Brown. Multiple linear regression analysis: A matrix approach with matlab. Alabama Journal of Mathematics, 2009.

[11] Alawode A. olaide, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control Pages 85–90, 2009.

[12] Himeldev, Tanmoysen, Security and privacy implications of data mining. In ACM SIGMOD Workshop, pages 15–19, 1996.

[13] Kangchan Lee : Security Threats in Cloud Computing Environments. In International journal of security and its applications, October, 2012, Vol. 6, No. 4.

[14] Neha Tirthani: Hellman and elliptical curve cryptography, Proceedings of TCC, volume 3378 of LNCS, pages 325-341. Springer-Verlag (2005)

[15] Amar Gondaliya : Security in Cloud Computing, Technical Paper Contest 2011.

[16] Anthony Bisong, An Overview of the Security Concerns in enterprise Cloud computing, International Journal of the Security Concerns in Enterprise Cloud Computing, 2011.

[17] R. Kalaichelvi Chandrahasan, Research Challenges and Security Issues in Cloud Computing, International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3.

[18] Vahid Ashktorab, Security Threats and Countermeasures in Cloud Computing, International Journal of Application or Innovation in Engineering and Management, Vol 1, Issue 2, October 2012.

[19] Mandeep Kaur, Using encryption algorithms to enhance the data security in Cloud computing, International journal of communication and computer technologies, Vol 1, No 12, 2013.

[20] Mr. Tejas P. Bhatt, Security in Cloud Computing using File Encryption, International Journal of Engineering Research and Technology , Vol. 1 Issue 9, November 2012.

[21] Eng. Anwar J. Alzaid and Eng. Jassim M. Albazzaz, "Cloud Computing Challenges and related Security Issues", 2009 A sur vey Paper http://www.cse.wustl.edu/~jain/cse571- 09/ftp/cloud/index.html

[22] A. Raja Rajeswari and R.Sakkaravarthi , "Top Threats to Cloud Computing V1.0" , March 2010