International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 6, ISSN No. 2455-2143, Pages 47-51
Published Online April - May 2016 in IJEAST (http://www.ijeast.com)

A SURVEY ON MINING ATTACKS ON CLOUD DATA AND SECURITY CHALLENGES

CH. Sekhar
Asst. Prof Dept. of CSE
Vignan's Institute Of Information Technology,
Duvvada, Visakhapatnam,
Andhra Pradesh

P. Ratna Kumari
Asst. Prof Dept. of CSE
Vignan's Institute Of Information Technology
Duvvada, Visakhapatnam,
Andhra Pradesh

Abstract: Cloud computing is an emerging technology to provide resources from the large data centers. Cloud technology 0 is made available as a service to the users. +- It has become prominent IT to start a business or to utilize the resources without any capital investment. Cloud services are "pay-per-use" over the internet. It is on demand access to virtualized IT services and products. Rackspace, Salesforce, Amazon, Google, IBM, Dell and HP are the well known service providers. There are important issues that need to be mention with respect to sensitive, valuable data security and privacy in a cloud environment.
Data mining refers to extracting or "mining" knowledge from large amounts of data which was previously unknown and potentially useful information by efficient knowledge discovery techniques. Data mining has been a popular research area for more than a decade due to its vast spectrum of applications. The power of data mining tools to extract hidden information that cannot be otherwise seen by simple querying proved to be useful.
One of the security problems in cloud computing is mining based attacks, may extract the data by using mining tools and continuously by an unanonymous person to get the sensitive information. This paper focusing and mentions detailed analsis of the various threats and security issues threatening the cloud computing adoption.

I. INTRODUCTION

Internet has been a common platform to all to learn use the various technologies that have been developed since it started. Important among all of them is *Cloud Technology*. Over the past decade of years, cloud computing technology has witnessed a tremendous shift towards its adoption and it has become a emerging technology in the information technology space as it promises significant cost reductions and improving the new business startup potential to its users and providers. The main boost of using cloud computing will include: i) minimized hardware and maintenance cost, ii) accessibility around the universal ,iii) simplified flexibility and highly automated processes wherein the customer need not worry about any kind of software up-gradation. Cloud is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In such an environment users need not own the infrastructure for various computing services. Customer can have chance to they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi-tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their problem.
The cloud computing technologies having services include Software as a Service (SaaS), Platform as a

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 6, ISSN No. 2455-2143, Pages 47-51
Published Online April - May 2016 in IJEAST (http://www.ijeast.com)

Service (PaaS), and Infrastructure as a Service (IaaS) Data Base as Service (DaaS). Using the cloud computing services, users are able to export their data in servers and access or import their data from anywhere and they need not worry about the loose of data due to disk faults, system breakdown etc.

There are various analysis tools and techniques for data retrieval are available now to expose the sustainable data and sensitive information from cloud data. The non-customers or unauthorized persons can use these tools to get the sensitive data from cloud storage. Now a days that getting valuable information from a huge volume of data. These analysis techniques are being used by cloud service providers. For example, Google uses data analysis techniques to analyze user behaviors and recommend search results. Attackers can use these techniques to getting valuable data from the cloud. The recent trends of data analysis Data mining can be a potential threat to cloud security considering the fact that entire data belonging to a particular user is stored in a single cloud provider. The single storage provider approach gives the provider opportunity to use powerful mining algorithms that can extract private information of the user. As mining algorithms require a reasonable amount of data, the single provider architecture suits the purpose of the attackers. This approach (single cloud storage provider) also eases the job of attackers who have unauthorized access to the cloud and use data mining to extract information. Thus the privacy of data in the cloud has become a major concern in recent years.

II. DATA MINING ASSOCIATED WITH CLOUD

Data mining is carried out over huge volumes and velocity of data in order to extract "new information out of them that will be the basis for making (better) business decisions and needs DM is highly multidisciplinary field, which has its roots in statistics, mathematics, information theory, artificial intelligence, machine learning theory, data bases and in the whole series of other related fields. DM involves activities of searching from Data Warehouse and huge data base with the aim to find the sensitive and hidden, so far unknown facts, regularities or patterns. Data mining represents finding useful patterns or trends through large amounts of data warehouses. Data mining tools predict future trends and behaviors, allowing businesses to make proactive, knowledge-driven decisions.

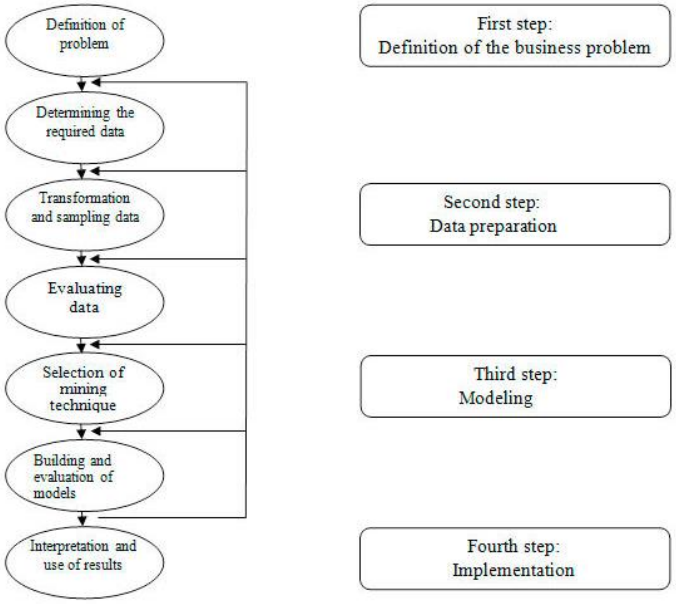

Fig2.1Data Mining Process steps

2.1Data Mining Techniques:

Various techniques will be used to extract the hidden data from data warehouse. The following are

- **Classification:** classification is used to classify each item in a set of data into one of a predefined set of classes or groups. Uses techniques like decision trees, linear programming, neural network and statistics.
- **Clustering**: cluster of objects which have similar characteristics using the automatic technique. Members of a cluster are having similar property or behavior
- **Association**: finding the relation among the attributes. Item or pattern is discovered based on a relationship and bonding between items in the same transaction.
- **Outer layer**: Pattern can be find if the pattern not fit into any of the group or class.

2.2Cloud Computing:

The Cloud, as it is often referred to, involves using computing resources – hardware and software – that are delivered as a service over the Internet. Cloud computing represents both the software and the hardware delivered as services over the Internet. Cloud Computing is a new concept that defines the use of computing as a utility, that has recently attracted significant attention.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 6, ISSN No. 2455-2143, Pages 47-51
Published Online April - May 2016 in IJEAST (http://www.ijeast.com)

NIST defines cloud computing as a model that provides ubiquitous, simple and on demand network access to a shared set of resources (e.g. network resources, servers, data storage, applications and services) that can be readily available for use or if necessary shut down and **all with minimal intervention of service providers.**
This cloud model is composed of five essential characteristics, three service models, and four deployment models." The essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.
The service models that compose cloud computing are:

2.3Cloud Computing – Characteristics:
The 5-4-3 of cloud computing

5. Characteristics:

- Elastic Resources
- IT Service Centric approach
- Consumption based metering
- Self service ubiquitous network access
- Location independent resource pooling

4- Deployment Model:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud

3-Service Offering Models

- Software as a Service(SaaS),
- Platform as a Service(PaaS),
- Infrastructure as a Service(IaaS)

III. CLOUD COMPUTING CHALLENGES IN SECURITY

The major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:
It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Well-known security issues such as data loss, phishing, and botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnetas Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value, reports the 2012 Computerworld "Cloud Computing" study, which measured cloud computing trends among technology decision makers. When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility into sensitive data.
There are complex data security challenges in the cloud:

- The need to protect sensitive business, government, or regulatory data.
- Cloud service models with multiple tenants sharing the same infrastructure.
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Auditing, reporting, and compliance concerns.
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT. security intelligence and risk management

Specific security challenges pertain to each of the three cloud service models:

- SaaS: Service levels, security, governance, compliance, liability expectations of the service & provider are contractually defined

- PaaS, IaaS: Customer sys_admins manage the same with provider handling platform, infrastructure security.

3.1 Cloud Computing Security and Analysis:

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from direct accessing the shared data, proxy and brokerage services should be employed.
The response to a familiar set of security challenges that manifest differently in the cloud. New technologies and fuzzier boundaries surrounding the data center require a different approach.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 6, ISSN No. 2455-2143, Pages 47-51
Published Online April - May 2016 in IJEAST (http://www.ijeast.com)

- A set of rules, technologies, and controls designed to protect data, infrastructure, and clients from attack and enable regulatory compliance.
- Layered technologies that create a durable security net or grid. Security is more effective when layered at each level of the stack.
- About providing protection whatever delivery model you deploy or use: private, public, or hybrid cloud environments.
- The joint responsibility of your organization and your cloud service provider(s). Depending on the cloud delivery model and services you deploy, security is the responsibility of both parties.

Major Trends That Impact Cloud Security

To organize cloud security in now a day's world, you need a solution that helps you address threats to enterprise data and infrastructure, including the major trends you are up against.

1. Changing attackers and threats: Threats are no longer the purview of isolated hackers looking for personal fame. More and more, organized crime is driving well-resourced, sophisticated, targeted attacks for financial gain. Plus cybercriminals have expanded their attack targets from just software to the platform.

2. Consumerization of IT: As smart devices mobiles, tabs and technologies continue to proliferate, customer want to use personally owned devices to access enterprise applications, data, and cloud services.

3. Evolving architecture technologies: With the huge increase of virtualization and the use of public/Hybrid clouds, perimeters and their controls within the data center are in flux, and data is not easily constrained or physically isolated and protected. Cloud technologies methods present new way if security challenges; for example, API management and governance is a critical discipline for enterprises to scale delivery of cloud services to mobile and other clients.

4. Dynamic and challenging regulatory environment: Organizations—and their IT departments—often face ongoing burdens of legal and regulatory compliance with increasingly prescriptive demands and high penalties for noncompliance or breaches. Commonly cited examples of regulations include Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the Data Protection Act in the United Kingdom, and the European Union (EU) Data Protection Directive.

IV. ANALYSIS OF SECURITY SELECTION CRITERIA AND CONSIDERATIONS:

Key Point	**Measure**
Data center risk management and security practices	• Various patch management techniques and methodology? • How does technology architecture and infrastructure impact the cloud service provider's ability to meet SLAs?
Hardware Equipments -based security	• Can the cloud service provider offer trusted pools for your most sensitive workloads? • Is encryption a software-only solution?
Technology segmentation	• Way in which systems, data, networks, management, provisioning, and personnel segmented? • Whether they can be controls segregating each layer of the infrastructure properly integrated so they do not interfere with each other? For example, investigate whether the storage compartmentalization can easily be bypassed by management tools or poor key management. • What cloud access and identity protocols are used?
Identity and access management	• How is identity managed and authenticated? • Is two-factor authentication utilized?
Secure connections	• How are connections that transfer data secured?
Attack response	• How are attacks monitored

and recovery	and documented? • How quickly can the cloud service provider respond? • What recovery methods are used?
Compliance capabilities	• Is the cloud service provider have the ability to comply with regulatory requirements that you face? • Whether the cloud service provider able to provide you with full visibility into compliance-related activities? • Can you perform your own audit?
System availability and performance	• In what way the various cloud service provider handle resource democratization and dynamically to predict proper levels of system availability and performance through normal business fluctuations? • In what way the cloud service provider measure performance?

V. REFERENCES

[1] Peter Mell and Timothy Grace, "The NIST Definition of CloudComputing", *National Institute of Standards and Technology Gaithersburg*,Special Publication 800-145, January 2011.

[2] Lijun Mei, W.K. Chan and T.H. Tse, "A Tale of Clouds:Paradigm Comparisons and Some Thoughts on Research Issues", *IEEEAsia-Pacific Services Computing Conference*, 2008, pp 464-469.

[3] "Amazon Auto Scaling in Cloud Computing",http://aws.amazon.com/autoscaling/30.05.2012

[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] Security and Mutual Trust in Cloud Computing Storage Systems, 1Shaik Meer Subhan Ali, Ch. Sekhar, IJCST Vol. 5, Iss ue 4, Oct - Dec 2014

[7] Ruxandra-Ştefania PETRE, "Data mining in Cloud Computing", Database Systems Journal vol. III, no. 3/2012

[8] Ch.Sekhar, U Nanaji- "Secure Cloud by IT Auditing" Inte

[9] Data Mining Book by Kamber

[10] TPA Based Public Auditing for Data Storage Security in Cloud Computing, Karuna G, K. Ravindra,IJCST Vol. 3, Iss ue 3, July - Sept 2012