Security Issues in Cloud Computing: An Overview

Anupama Chowdhary
Principal, Keen College
Bikaner (Rajasthan)
India

Abstract **–** Cloud Computing allows the exploitation of all available resources on the Internet in a scalable and simple way. As the cost of the information processing and Internet accessibility falls, more and more organizations are opting cloud services. The cloud service layers and multi contract virtual architecture create a complex environment, so it is difficult to develop and manage an information security. On the other hand it is becoming vulnerable to a wide variety of cyber threats to the security of the company's data and information. Security on Clouds can be obtained via Intrusion Detection System (IDS) or Security Operations Centre (SOC).

Index terms **–** cloud computing, Security Operations Centre (SOC), Intrusion Detection System (IDS), SLA (Service Level Agreement).

I. INTRODUCTION

Security is the major problem in clouds, as one cannot know how safe outsourced data is and when using these services ownership of data is not always clear. There are also issues regarding policy and access of data. Cloud providers use data mining to provide clients a better service [1]. If clients are unaware of the information being collected, ethical issues like privacy and individuality are violated [2][3]. Attackers outside cloud providers having unauthorized access to the cloud, also have the opportunity to mine cloud data. In both cases, attackers can use cheap and raw computing power provided by cloud computing [4][5] to mine data and thus acquire useful information from data. So in general we can state there are security issues for

- Policy and access of data as if customer's data is stored abroad then FOI (Freedom of Information) policy of which country will be applicable.
- Cloud providers can misuse mined data.
- Attackers outside the cloud my misuse data mining tool such as, analysis of GPS data can be used to create a comprehensive profile of a person covering his financial, health and social status [6], clustering algorithms can be used to categorize people or entities and are suitable for finding behavioral patterns, multivariate analysis identifies the relationship among variables and this technique can be used to determine the financial condition of an individual from his buy-sell records, clustering algorithms can be used to categorize people or entities and are suitable for finding behavioral patterns, association rule mining can be used to discover association relationships among large number of business transaction records [7]. Data in cloud can be effectively secured by encrypting it. Direct access of client can be restricted by using proxy and brokerage services [8].

From an architectural perspective, there is a thin line between conventional computing and cloud computing. However, cloud computing will impact the organizational, operational, and technological approaches to data security, network security, and information security good practice [9].

II. SECURITY CONSIDERATIONS

Organizations using cloud computing to store or process publicly available data consider the availability and integrity of the public data and may not be concerned about confidentiality. Moreover, organizations focus on their core business, the acquisition and maintenance of specialist IT staff, computing software and hardware used to store and process data can be outsourced to a vendor. Organizations thus consider the following points while outsourcing

- The contract between a vendor and their customer must address security risks, and cover who has access to the customer's data and the security measures used to protect the customer's data. Vendor's responses to important security considerations must be apprehended in the Service Level Agreement, otherwise the customer only has vendor promises and marketing claims that can be hard to verify and may be unenforceable.
- In some cases it may be impractical or impossible for a customer to personally verify whether the vendor is following the contract or not. So the customers have to rely on third party audits and their certifications. Customers should consider which of the vendor's certifications are useful and relevant, how much the certification increases the customer's confidence in the vendor, what associated documents the customer can request from the vendor, and whether the contents of the documents are of high quality.
- Considerations should be made to protect data from unauthorised access by
  - ✓ a third party.
  - ✓ the vendor's customers.
  - ✓ some of vendor's employees.

In SaaS environments the security controls and their scope are negotiated between customer and service provider at the time of signing SLA (Service Level Agreement). Service levels, privacy, and compliance are all issues to be dealt with legally in contracts. In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility. PaaS offers a balance somewhere in between, where securing the platform itself falls onto the provider, but securing the applications developed against the platform and developing them securely, both belong to the consumer. The security responsibilities of both the provider and the consumer greatly differ between cloud service models. For example

- Amazon [10] provide cloud computing and storage services EC2 and S3. EC2 IaaS offering includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for security controls that relate to the IT system including the operating system, applications, and data. The security of EC2 and S3 is based on ensuring that user's virtual machines are well separated from each other, and that Amazon servers are protected from being directly controlled by these machines.
- Salesforce.com's customer resource management (CRM) SaaS offering is not only responsible for the physical and environmental security controls, but it must also address the security controls on the infrastructure, the applications, and the data.
- IBM cloud security is based on Service Oriented Architecture model [11]. The model allows cloud users to choose which security services they need, and in what configuration. The model is supported by the Web Services (WS) framework. IBM Security Policy Manager can be used by cloud users to write and enforce data access policies. IBM AppScan can be used to monitor user applications.
- Microsoft approach focuses on planning risk, designing security controls and ensuring compliance [12]. Compliance framework is used to monitor and evaluate security controls to ensure they are operating as required. The framework verifies that security controls meet industry and governmental standards. In addition, security incident management is used to identify attacks, contain the attacks, mitigate them and recover from these attacks.

Securing and moderating risks to cloud assets has been a long-standing concern for cloud security teams. Vendors have developed an array of technologies, like Firewalls, IDS/IPS, Anti-Virus/Anti-Malware, and so on. Over time, organizations have set up Security Operations Centers (SOCs) to help manage these technologies. In this paper Intrusion Detection System (IDS) and Security Operations Centers (SOC) are discussed.

III. INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system (IDS) is combination of hardware and software elements that work together and monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is reported either to an administrator or collected centrally. This central system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms. If it finds unexpected events that may indicate an attack will happen, is happening, or has happened. An IDS also watches for attacks that originate from within a system.

Kabiri and Ghorbani [13] and Sobh [14], have mentioned that several IDS approaches have been proposed in the specialized literature since the origins of this technology, two highly significant works in this direction are Denning [15] and Staniford-Chen et al. [16]. Remarkable work has been carried out by a working group known as CIDF (Common Intrusion Detection Framework) created by DARPA in 1998. Its main orientation was towards coordinating and defining a common framework in the IDS field. Integrated within IETF in 2000, and having adopted the new acronym IDWG (Intrusion Detection Working Group), the group defined a general IDS architecture based on the consideration of four types of functional modules

- E blocks (Event-boxes): This kind of block is composed of sensor elements that monitor the target system, thus acquiring information events to be analysed by other blocks.

- D blocks (Database-boxes): These are elements intended to store information from E blocks for subsequent processing by A and R boxes.

- A blocks (Analysis-boxes): Processing modules for analysing events and detecting potential hostile behaviour, so that some kind of alarm will be generated if necessary.

- R blocks (Response-boxes): The main function of this type of block is the execution, if any intrusion occurs, of a response to stop the detected threat.

IDS solutions detect threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations but lack the visibility into application layer of TCP/IP stack and hence may not protect from application specific attacks.

IV. SECURITY OPERATIONS CENTRE (SOC)

A security operations center (SOC) is a centralized facility that deals with security issues on an organizational and technical level. SOC have an information security team responsible for monitoring and analyzing an organization's security on an ongoing basis. The SOC team is armed with technology solutions and a strong set of processes to detect, analyze, and respond to cyber security incidents quickly upon discovery. The effectiveness of SOC depends upon the strategy defined to address the essential functions such as:

- Monitoring: The best way to prevent security threats is to monitor threat data and determine where possible security events must be investigated. For the purpose SOC have to decide
  - Specific data to be monitored:
    - Within set hours or around the clock.
    - Agreement and regulation that permit specific data monitoring.
  - Security events/incidents to be monitored:
    - In near-real time.
    - Type of event-monitoring tool needed and flow of data in these tools.
    - Tuning flow of events for better results.
    - Type of monitoring reports needed and who will use it.
    - Updating for new technology and threats/events.
    - Detection of event sources and logs that stop flowing to the monitoring tools.
  - Human resources:
    - Skill development.
    - Motivation and education.
    - Providing right amount of information for effective decision making.
- Incident management: This function defines which security incidents demand a response and what necessary actions are to be taken to remediate the risk. So SOC have to decide
  - The policies for the security devices and their testing.
  - Authorization to make changes in policies, periodical reviews the overall policies.
  - Updation of security definition files, software and firmware.
  - Fault tolerance required for gateway and inline devices.
  - Access policies for the devices to third parties and others.
  - Coordination of monitoring and policy team for tuning of devices.

  Normally an integrated ticketing system is used to capture the threat analysis, process it as a security incident, and track that the necessary remediation actions have been taken.
- Defining process and procedures: A process defines who will do a specific task and a procedure defines how that task actually gets done. The processes and procedures are defined for detecting and remediating security issues, administrative and management duties, system administration, maintenance and management and day-to-day operations.
- Personnel recruitment, training and management: The recruited staff will be the heart and soul of SOC. For their better performance their training and education for the particular technology used is also important. Moreover shifts should be scheduled and their responsibilities for each position and for each scheduled shift should be defined.
- Strategy: The threat strategy should be evolving that is latest security intelligence should be used. If this is not done the data will be exposed to hackers or malware and SOC will never know about it.

Figure 1 Developing Security Operations Centre (SOC)

In response to the ever-changing security threat landscape SOC components and expected services has changed over time. There are four incremental generations of SOC [17].

- First-Generation: The basic features were – device monitoring, log collection and retention, limited device coverage, slow reaction to security incidents.
- Second Generation: Additional features were – events correlation, network and syslog log collection case management.
- Third Generation: Additional features were – vulnerability management, incident response capabilities.
- Fourth Generation: Additional features are – data correlation, big data security analytics, threat intelligence services, consumption of cloud security services, network flow analysis, and digital investigation.

A Security Operation Center (SOC) is made up of five distinct modules: event generators, event collectors, message database, analysis engines and reaction management software.

Event Generators: There are two types of event generators

1. Event based data generators / Sensors – which generate events according to a specific operation performed on the OS, applications or over the network. Mostly used sensors are IDS's or any filtering system providing

logging such as firewalls, routers with ACLs, switches and Wireless HUBs implementing MAC address restriction, RADIUS servers, SNMP stacks, etc. Each sensor should be fault tolerant, impose a minimal overhead, run continually, resist subversion, be configurable & adaptable, be scalable, provides graceful degradation of service and allow dynamic reconfiguration [18].

2. Status based data generators / Pollers – which generate an event according to the reaction to an external stimulus such as ping, data integrity checking or daemon status check. It may be difficult to setup systems that would be able to poll hundreds of targets at short intervals whilst non-disturbing the managed systems operations.

Event Collectors: Its purpose is to gather information from different sensors and translate them into a standard format, in order to have a homogeneous base of messages.

Message Database: They perform a basic level of correlation in order to identify and remove duplicates either from the same or different sources. It is also responsible for database availability, integrity and confidentiality. Sensors may generate dozens of messages each second those messages will have to be stored, processed and analyzed as quickly as possible, in order to allow a timely reaction to intrusion attempts or success.

Analysis Engines: Correlation, structural analysis, intrusion path analysis, behavior analysis etc. techniques is used to generate alerts.

Reaction management software: Reaction ranges from passive monitoring for further information through to target system emergency halt through CERT incident reporting [19]. Appropriate reaction should be determined before an attack takes place and procedures must be validated then securely stored and made accessible to supervision teams.

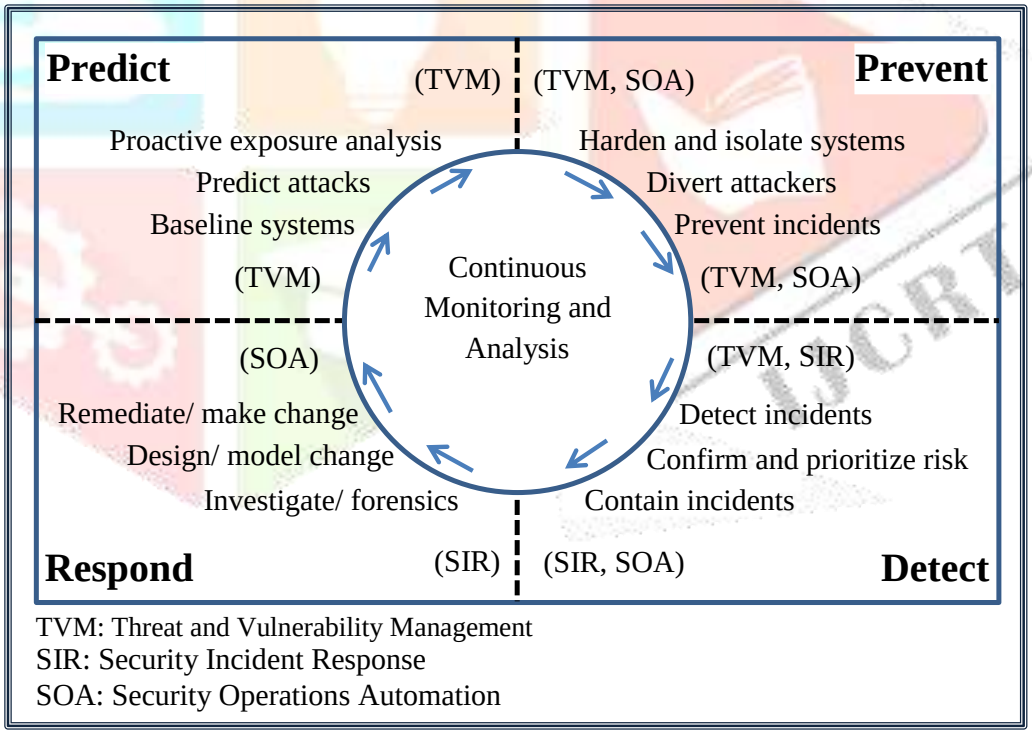

Figure 2 Intelligence-Driven Security Operations Centre

Mostly SOC uses signature-based approaches, the traditional prevention mechanisms, and security controls; so many current attacks bypass it. Gartner [19] surveyed organizations with SOC capability, among those enterprises 82% stating the same problems. Gartner's adaptive security architecture outlines four critical domains: prevent, detect, respond and predict (Figure 2). For a SOC to be effective at detection and response, it needs to continuously evolve and adapt to changes in the technology and threat environment. For rapid response, as much of the mundane work should be as automated as possible, and other human-augmented responses should be aided with decision support systems. Gartner [20] outlines five models for SOC: Virtual

SOC, Multifunction SOC/NOC, Co-managed SOC, Dedicated SOC and Command SOC. In virtual SOC there is a virtual team who become active in cases of incidents. Multifunction SOC/NOC has a dedicated team, facility, and infrastructure that do more than security, including IT operations, compliance, and risk management. Co-managed SOC model has typically an 8×5 operation with 24×7 monitoring for organizations not having core expertise in IT or security operations. Dedicated SOC is a centralized SOC that has a dedicated infrastructure, team, and processes. Command SOC controls other SOCs and is more focused on managing threat intelligence and situation awareness than day-to-day operations.

V. CONCLUSION

In the current world of internet, the number and complexity of malicious events are increasing day-by-day. Security is one of the main concerns for cloud-computing applications, since user data and/or applications become a great target for such events. We have gone through two mechanisms for handling security issues in cloud computing. IDS solutions detect threat activity in the form of malware, spyware, viruses, worms, and other attack types and threats posed by policy violations but it may not protect from application specific attacks. So for better solutions we move on to SOC. The success of SOC majorly depends upon the SOC analyst, and management team. SOC analyst must be extremely curious, abstract thinker, ethical and patient to handle frustrating situations. We have also discussed the model developed for various types of organizations by Gratner. For cloud providers a dedicated SOC model should be adopted to provide secure transactions to clients. Moreover SOC as a service could also be provided by clouds.

References

[1] J. Wang, J. Wan, Z. Liu, and P. Wang. Data mining of mass storage based on cloud computing. In IEEE Computer Society, pages 426–431, 2010

[2] L. Van Wel and L. Royakkers. Ethical issues in web data mining. Ethics and Inf. Technol., 6:129–140, 2004

[3] C. Clifton and D. Marks. Security and privacy implications of data mining. In ACM SIGMOD Workshop, pages 15–19, 1996

[4] R. Chow, 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.

[5] L. Li and M. Zhang. The strategy of mining association rule based on cloud computing. In IEEE Computer Society, pages 475–478, 2011.

[6] W. Karim. The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring. Washington University Journal of Law and Policy, 14:485– 515, 2004

[7] Y. Liu, J. Pisharath, W. keng Liao, G. Memik, A. Choudhary, and P. Dubey. Performance evaluation and characterization of scalable data mining algorithms abstract

[8] Anuja R.Yeole, Poonam Borkar, “Survey Paper on Data Mining in Cloud Computing”, International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064.

[9] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0," Cloud Security Alliance. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[10] Amazon Web Services: Overview of Security Processes. Amazon, Sep 2008. Retrieved December 2010, from aws.amazon.com.

[11] IBM Point of View: Security and Cloud Computing. IBM, Nov 2009. Retrieved December 2010, from www-03.ibm.com/security/cloud-security.html

[12] Securing Microsoft Ss Cloud Infrastructure. Microsoft, May 2009. Retrieved December 2010, from www.globalfoundationservices.com/security

[13] Kabiri P, Ghorbani A. A., Research in intrusion detection and response – a survey. International Journal of Network Security 2005;1(2):84–102.

[14] Sobh TS. Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces 2006;28:670–94.

[15] Denning ED. An intrusion-detection model. IEEE Transactions on Software Engineering 1987;13(2):222–32

[16] Staniford-Chen S., Tung B., Porrar P., Kahn C., Schnackenberg D., Feiertag R., et al. The common intrusion detection frameworkdata formats. 1998. Internet draft 'draft-staniford-cidf-dataformats-00.txt'

[17] Joseph Muniz, Gary Mchntyore, Nadhen AlFardan, "Security Operations Center, Building, operating and maintaining your SOC", Ciscopress.com.

[18] Eugene H. Spafford, Diego Zamboni, Intrusion detection using autonomous agents, Computer Networks 34 (2000) 547-570.

[19] The Five Characteristics of an Intelligence-Driven Security Operations Center, Gartner 02 November 2015 | ID:G00271231

[20] Gartner Report: The Five Models of Security Operation Centers Oct 17, 2016 Whitepaper