IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

Security in Cloud Computing using IDS

Simranpreet Kaur[1], Manvi Chauhan[2] and Ankita[3]
Assistant Professor, Department of Computer Science[1]
UG Student, Department of Computer Science[2,3]
Dronacharya Group of Institutions, Greater Noida, India

Abstract: *The market growth is primarily focusing on the implementation and investment in various cloud based projects as the rise in demand for cloud based platforms has been a benefit for cloud based vendors creating opportunities in expansion of the business by launching various editions and advanced version for better productivity. The global cloud computing market is projected to grow from $250.04 billion in 2021 to $791.48 billion in 2028 at a CAGR of 17.9% in the forecast period The growth is attributable to the digital transformation, increasing penetration towards connected devices and growing automation amongst small and medium enterprises. Unforeseen emergencies, application vulnerabilities and online cyber attacks are the various restraining factors for Privacy & Security Concerns about data breaches and data losses. With the requirement of faster processing cycle in real time scenario, various enterprises are moving towards Omni-Cloud Solutions to leverage numerous advantages such as ease of data use, effective decision making , scalability and security of data. The trending protective method applicable here is Intrusion Detection System, which is one the way for real-time detection for breaches and establishment of more stronger security.*

Keyword: Cloud Computing, Data Security, Intrusion Detection , Privacy, Risks and threats**.**

I. INTRODUCTION

In recent years, cloud computing deemed to be the most emerging internet based technology in (IT)Information Technology world. It grew rapidly until it became preferred choice of every individual and organisation involved with its new computing and communication paradigms. It offers scalable and virtualized resources. These resources such as storage, information, platforms, servers are provided to cloud users as services on demand. This pay -per use makes it possible for many organization to avoid capital expenditure.

The current trends for the IDS is far from a reliable protective system, but instead the main idea is to make it possible to detect novel network attacks. One of the major concerns is to make sure that in case of an intrusion attempt, the system is able to detect and report it. Once detection is reliable ,next step would be to protect the network. In other words ,the IDS system will be upgraded to an Intrusion Detection and Response System (IDRS).

II. CLASSIFICATION OF IDS

IDS looks for attack signatures, which are specific patterns that usually indicates malicious or suspicious intent. It is based on

- Anomaly Detection
- Signature Based Misuse
- Host Based
- Network Based
- Stack based

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

2.1 Anomaly based IDS

This IDS models the normal usage of the network as a noise characterization. The two phases of a majority anomaly detecting systems consist of training phase and testing phase (where current traffic is compared with the profile created in training phase).These are detected in many ways such as system using artificial neural networks are used to a great effort .It also defines normal usage of the system comprises using a strict mathematical model, and flag deviation from this as an attack .This is known as strictly anomaly detection .Some other techniques used to detect include data mining ,grammar based methods.

A. Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

2.2 Signature based IDS

This IDS possess an attacked description that can be matched to sensed attack manifestations. It also recognizes bad patterns such as malware .It monitors the packet traversing the network, compares these packets to the database of known IOCs or attack signatures to flag any suspicious behaviour whereas anomaly can alert you to suspicious behaviour that is unknown.

ID is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets ,as an attack. For example ,an IDS that watches web servers might be programmed to look for a string "phf" as an indicator of a CGI program attack.

A. Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms.
- Have to programmed again for every new pattern to be detected.

2.3 Host/Application based IDS

The host operating system or the application logs in the audit information. These audit information includes events like the use of identification and authentication mechanism (logins etc.), file opens and program execution ,admin activities etc. It monitors the computer infrastructure on which it is installed, analyzing traffic and logging malicious behaviour. It also gives deep visibility into what is happening on your critical security systems. This audit is then analyzed to detect trails of intrusions.

B. Drawbacks of Host based IDS

- The kind of information needed to be logged in as a matter of experience .
- Unselective logging of messages may greatly increase the audit and analysis burdens .
- Selective logging runs the risk that attack manisfestations could be missed.

C. Strengths of host based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments.
- Monitoring key components.
- Near Real-Time detection and response.
- No additional hardware.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

2.4. Stack based IDS

They are integrated closely with IP stack ,allowing packets to be watched as they traverse their way up the OSI layers.This allows the IDS to pull the packets from the stack before the OS or the application have a chance to process the packets.

2.5. Network based IDS

This IDS looks for attack signatures in network traffic via a promiscuous interface. A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module.

A. Strengths of Network based IDS

- Packet analysis
- Malicious intent detection
- Complement and verification

2.6 Future of IDS

Developing IDS schemes for detecting novels attacks rather than individual instantiations.

3. HINDERANCE IN CLOUD

Many of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are:

1. Privileged User Access Management
2. Regulatory Compliance,
3. Data Location,
4. Data Segregation,
5. Data Protection and Recovery Support,
6. Investigative Support, and
7. Long-term Viability.

It is highly recommended that these questions, along with other risks, are assessed and addressed. Some of the assessments could be as follows:

1. Organization capability and maturity
2. Technology & data risks
3. Application migration and performance risk
4. People risks
5. Process risks
6. Policy risks
7. Extended supply chain risks

IV. CLOUD SERVICE MODEL

There are three main types of cloud computing services, sometimes called the cloud computing stack because they build on top of one another.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

4.1 (IAAS) Infrastructure as a Service

Used for Internet-based access to storage and computing power. The most basic category of cloud computing types, IaaS lets one rent IT infrastructure - servers and virtual machines, storage, networks and operating systems - from a cloud provider on a pay-as-you-go basis.

4.2 (PaaS) Platform as a Service

Enables developers with the tools to build and host web applications. PaaS is designed to give users access to the components they require to quickly develop and operate web or mobile applications over the Internet, without worrying about setting up or managing the underlying infrastructure of servers, storage, networks and databases.

4.3 (SaaS) Software as a Service

Used for web-based applications. SaaS is a method for delivering software applications over the Internet where cloud providers host and manage the software applications making it easier to have the same application on all of your devices at once by accessing it in the cloud.

V. Cloud Deployment Model

The three most common types of cloud deployment models are Private Cloud, Public Cloud, and Hybrid Cloud.

5.1 Private Cloud

In this deployment model, the resources are dedicated to a single or a set of organizations and treated as an intranet functionality. The billing usually is on a subscription basis with a cloud consumer making minimum commitments.

A. Implications

Positive security implications are relatively high and the organization has significant influence on the architecture, processes, and tools used in the deployment**.**

B. Challenges

Security challenges include high cost of implementation and management, skills requirement, and vulnerability management. In this deployment model, cost and return on investment are key factors and the security implementation is usually based on risk assessment and hence, the security cover is not comprehensive.

5.2 Public Cloud

In a public cloud, resources are dynamically committed on a fine-grained, self-service basis over the Internet or a portal10. Billing is usually consumption-based and is charged on a pay per use basis

A. Implications

The cloud service provider normally has a comprehensive & layered security system, which can potentially provide a high degree of security due to its implement once and use multiple times model, which significantly reduces the cost of security implementation for the consumer.

B. Challenges

Security challenges are heightened, as the resources are not committed but leveraged across multiple cloud consumers. This not only adds additional burden of ensuring all applications and data accessed on the public cloud, but also has to manage the multitude of external influences such as legislative, data protection etc.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

5.3 Hybrid Cloud

Hybrid cloud is a deployment model where a private cloud is linked to one or more external cloud services while being managed centrally. It provides the cloud consumers a flexible and fit-for-purpose solution with a relative ease of operations

A. Implications

Positive security implications are that security can be purpose-built for vulnerabilities, threats, and risks that are assessed. This makes it cost-effective and targeted

B. Challenges

Security challenges are relatively high as the deployment model is complex with heterogeneous environment, multiple orchestration, and automation tools.

VI. Need for Security Evolution

Cloud computing due to its disruptive nature, complex architecture, and leveraged-resources pose a unique and severe risk to all actors. It is critical to all stakeholders and actors to understand the risk and mitigate it appropriately. Security needs to be built at every layer in a cloud-computing platform by incorporating best practices and emerging technologies to effectively mitigate the risk. In the cloud, consumer, provider, broker, carrier, auditor, and everyone else has to take the necessary precautions against risks to truly secure the cloud-computing platform or be exposed to significant and sometimes business critical risk.

Work can be done to understand the challenges, requirements, and impact of effective security training for consumers and other providers.

VII. Risks and Security Concerns In Cloud Computing

7.1 Virtualization

Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system. It possess some risk to data in cloud that is compromising a hypervisor itself. Another risk with virtualization is associated with allocation and deallocation of resources. If VM data is written to memory and is not cleared before reallocation then there is a potential of data exposure.

7.2 Multitenancy

Shared access or multitenancy is also considered as one of the major risk to data in computing. As multiple users share same computing resources like CPU ,Storage or memory etc. it is a threat to multiple users. In such scenarios there is always a risk of private data accidentally leakinf to other users .If there is one fault in the system which allows another users or hackers to access all the other data.

7.3 Storage in Public Cloud

Storing data in public cloud is another security concern in cloud computing. Normally cloud implements centralized storage facilities, which can be appealing target for hackers. Storage resources are complicated systems that are combination of hardware an software implementations and cause exposure of data if a slight breach occurs in public cloud. In order to avoid such risks ,it is always recommended to have a private cloud if possible for extremely sensitive data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

VIII. Counter Measures and Control

- **End-to-end Encryption:** The data in a cloud delivery model might traverse through many geographical locations; it is imperative to encrypt the data end-to-end. Different cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring content integrity, authentication ,and availability .Using cryptography plaintext is encrypted into cipher text using an encryption key .
    - Block Ciphers is an algorithm for encrypting data in which a text cryptographic key and algorithm are applied to a block instead of per bit at a time.
- **Scanning for Malicious Activities**– End-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures to mitigate risks from malicious software passing through encryption.
    - **Example**: an administrator and managers of cloud services providers who can sometimes act as malicious agents and threatens the security of the clients using cloud computing applications.
- **Validation of Cloud Consumer**: The cloud provider has to take adequate precautions to screen the cloud consumer to prevent important features of cloud being used for malicious attack purposes.
- **Secure Interfaces and APIs**: The interfaces and APIs are important to implement automation, orchestration, and management. The cloud provider has to ensure that any vulnerability is mitigated.
- **Insider Attacks:** Cloud providers should take precaution to screening employee and contractors, along with strengthening internal security systems to prevent any insider attacks
- **Secure Leveraged Resources:** In a shared/multi-tenancy model, the cloud provider has secure shared resources such as hypervisor, orchestration, and monitoring tools.
- **Business Continuity Plans:** Business continuity plan is a process of documenting the response of the organization to any incidents that cause unavailability of whole or part of a business-critical process.

IX. Conclusion

Increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing the data in cloud. Data available in the cloud can be at risk if not protected in a rightful manner. This paper discussed about the Intrusion detection system ,its types and also discussed the risks and security threat to data in cloud and given an overview on security concern .Virtualization is examined to find out the threats caused by hypervisor. One of the major concerns of this paper was data security and IDS including its threats and solutions in cloud computing. .The study provided an overview of Intrusion System and encryption of data in cloud .

Acknowledgement

Foremost, We would like to express our sincere gratitude to our teacher, supervisor, mentor and our guide Prof. Simranpreet Kaur for the continuous support for research, for her patience, motivation, enthusiasm and immense knowledge. Her guidance helped us in all the time of research and writing of this paper. We could not have imagined having a better advisor and mentor for our study. The guidance and motivation she provided, helped us in exploring the topic and grabbing the opportunity to do the brain work out. This enhanced our knowledge as well as understanding the implication of it towards real time scenario. Therefore, leading the completion of the research efficiently.

References

[1]. Joarder Kamruzzaman, Ansam Khraisat, “Intrusion Detection System”, Article 20, 2019.
[2]. https://azure.microsoft.com
[3]. P.S. Wooley ,” Identifying Cloud Computing Security Risks, ”Contin . Educ. , vol. 1277, no. February , 2011.
[4]. https://www.sciencedirect.com

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2021
Impact Factor: 5.731

[5]. Vacca , John R. " Network and System Security", 26 August 2013 , ISBN 9781498702201.
[6]. https://www.fortunebusinessinsights.com
[7]. Cloud Security Alliance , "The Notorious Nine. Cloud Computing Top Threats in 2013 ," Security , no. February ,pp. 1-14,2013.
[8]. https://www.securonix.com
[9]. F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage ," pp. 1-6,2014.
[10]. Ion ,I . , Sachdeva, N., Kumarguru, P., S.(2011,July). Home is safer than the Cloud!:privacy concerns for Consumer Cloud storage . In Proceedings of the Seventh Symposium on Usable Privacy and Security(p. 130.ACM.
[11]. https://en.m.wikipedia.org
[12]. R. Sharma, R.K. Trivedi " Literature review: Cloud Computing – Security Issues, Solutions and Technologies International Journal of Engineering Research, 3(4)(2014),pp.221-225 [Google Scholar]
[13]. https://www.wikipedia.com
[14]. Gururaj Ramachandra," Survey on Security in Cloud Computing".