JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cloud Security Attack Detection Review Paper

Mr. Ashish Soni, Mr Rajneesh Pachouri, Mr. Anurag Jain, Ms.Charu Jain

M Tech Scholar, Assistant Professor, Assistant Professor, Assistant Professor, Assistant Professor
Department of Computer Science & Engineering
Adina Institute of Science & Technology, Sagar, India

Abstract: The adoption of cloud computing has been delayed, however, because there are still numerous technical problems with the features of cloud computing and the delivery of high-quality service. This review paper examines the security needs for cloud computing while highlighting the threats and difficulties related to cloud security. The main goal of this research is to categories the security risks and difficulties associated with the various types of cloud computing (SaaS, PaaS and IaaS).One of the most effective methods for hosting and delivering services over the internet has been touted as cloud computing. Cloud security is still a big worry for cloud computing, even with its broad range of applications. Many secure systems have been suggested to protect communication in such a setting, and the majority of them are based on attack signatures. These systems frequently struggle to effectively identify all forms of attacks. The new era of IT technologies has drawn attention to cloud computing due to the rising demand for services or utility computing on the global web. In order to offer strong processing and storage as on-demand services, one of the most difficult considerations is the security risk brought on by resource sharing over the cloud. Governments and companies all over the world are encouraged to create or migrate to the cloud in order to take advantage of the low cost resulting from the improvement in efficiency and performance made possible by cloud computing.

IndexTerms - Cloud Computing Security; Cloud Computing Risk.

I. INTRODUCTION

The ongoing expansion of the Internet has resulted in an increase in both the kind and frequency of computer attacks. Because they are becoming so significant, ransomware assaults and zero day exploits are receiving more media attention. Antivirus software and firewalls alone are no longer adequate to safeguard a company's network. IDS is one of the most important layers, created to shield its target from any potential threat by continually keeping an eye on the system (IDS). The two most common IDS now in use are anomaly detection and signature-based detection, often known as "misuse detection." In order to do signature-based detection, IDS data is compared to known attack patterns. This approach is utilised by many security solutions, but it has a significant drawback in that it can only detect threats that have already been documented in a database. When looking for anomalies in observed data, anomaly detection first creates a model of the game's typical behavior[1]. As a result, this technique produces a lot of false alarms even though it can identify undiscovered attacks.

In the context of cloud computing (CC), cloud security is seen as a crucial topic that has generated a lot of study.

In recent years, [2], [3], and [4]. For instance, a hacker might use CC's vulnerabilities to introduce a number of security risks, including denial-of-service attacks (DoS), DNS spoofing, and Address Resolution Protocol (ARP) attacks [5].

IoT tactics for collecting sensor data and creating intelligent applications and services have attracted a lot of attention in recent years. The Internet of Things (IoT) is defined as the process of connecting any object to the internet using integrated software and hardware that allows for data collection, exchange, and communication. The deployment of the Internet of Things makes the world much more accessible and offers an almost infinite variety of possibilities and interactions at home, at work, and during leisure time. By connecting sensors, devices, and people, the Internet of Things creates a kind of fluid interaction between hardware and software as well as between humans and machines. In the same way that networks and computer monitors are used on the internet to improve the element of organisations owing to the development of Machine learning and artificial intelligence, these interactions allow gadgets to anticipate, react, respond, and improve the physical world. By connecting sensors, devices, and people, the Internet of Things creates a kind of fluid interaction between people and technology, hardware, and software[6]. In the same way that networks and computer monitors are used on the internet to improve the element of organisational owing to development of Machine learning and artificial intelligence, these interactions allow gadgets to anticipate, react, respond, and improve the physical world.

IDS systems are particularly necessary in an IoT context because we anticipate an unprecedented number of attacks on numerous vital infrastructures [7]. The bulk of NIDS solutions that have been suggested use signature-based methods, which have several drawbacks [8]. For instance, behavioural changes must be simple to identify, evaluate, and attribute to particular network components (e.g. operating system versions, protocols or individual users). However, the variety of protocols and data that are transmitted over current networks make it difficult and complex for NIDS to identify intrusions [9]. It makes it more difficult to create a reliable baseline for attack detection in situations where the status of an online node must be periodically assessed to look for any signs of anomalous activity. Additionally, several of these systems raise questions about the rising degrees of human contact needed, which affects their efficacy.

The Trust-based Intrusion Detection and Classification System (TIDCS) and the Trust-based Intrusion Detection and Classification System-Accelerated (TIDCS-A) are two innovative systems that we suggest for secure networks in this study. The

proposed systems introduce the concept of periodic system cleaning, in which participant node trust connections are assessed and refreshed on a regular basis. Using a new feature selection algorithm, the method comprises deleting unnecessary and duplicate features. By controlling the number of iterations, the suggested technique can save time compared to exhaustive and heuristic search by randomly generating the features subset. So, a number of feature groups are chosen at random, and the effectiveness of the classifier is utilised as a criterion for evaluation. The selection of the groups is based on the optimal usage of the best qualities that will be grouped together for the machine learning algorithm to employ. In order to improve intrusion detection performance and network node trustworthiness while avoiding issues with minimal training data and dynamic behavioural node changes, a supervised machine learning method is integrated with historical data.

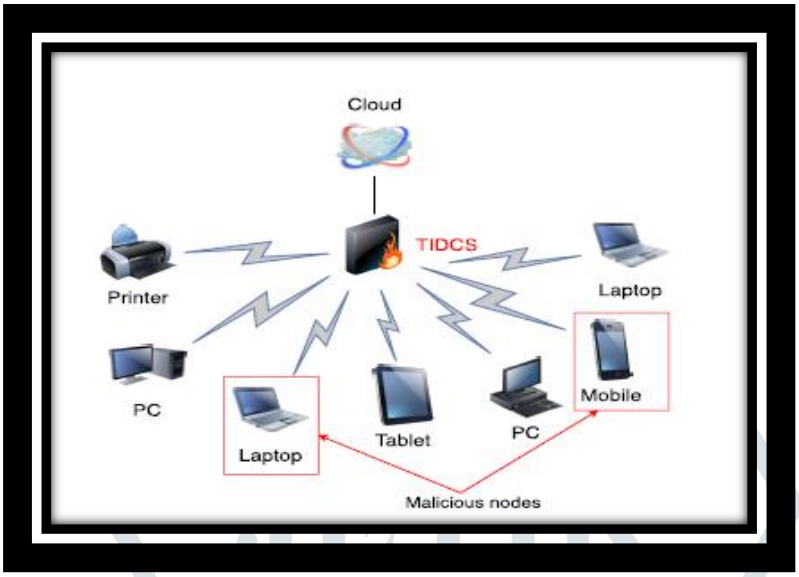

Figure 1TIDCS system model.

Intrusion Detection System (IDS)

Information security is built on the CIA triad, which originally stood for availability, honesty, and confidentiality. All unauthorised acts that impact any one, two, or all three of these information system components are referred to as cyber-attacks (or intrusions).

- The ISO 27000 standard defines confidentiality as "Property a certain data is not made available or divulged to unauthorised individuals, entities, or processes." In general, any information regarded as private, including credit card numbers, can be included in this data. Confidentiality must be maintained while allowing authorised users access to the data while prohibiting unauthorised users from doing so. A confidentiality breach results in data that cannot be rectified but can be controlled to affect consumers as little as possible. Confidentiality is implemented via a variety of security mechanisms, including encryption, passwords, two-factor authentication, security tokens, etc.[10]. The degree of secrecy of the information affects how well the appropriate security measures work. As a result, the same information can be protected using numerous levels of security that combine encryption and authentication techniques.
- Two more security solutions, firewalls and intrusion prevention systems, are commonly misunderstood for IDSs (IPSs)[11]. Each of these three security measures uses a different strategy to protect the systems inside a network. Firewalls, for instance, look for intrusions on the outside of the network and stop them before they reach the protected network. In order to filter incoming and outgoing traffic in accordance with specified criteria, packet headers are checked (protocol, IP address, port number...). IDSs, on the other hand, may monitor the protected network for any unusual activity occurring inside or outside of it. IDSs can't stop anomalous behaviour on their own, hence an administrator is required to manage the alarms they produce. This is not the case with IPSs, which carry out the same functions as an IDS but have the capacity to proactively stop an identified threat. This automation adds another level of complication because a subpar response could lead to additional network problems.

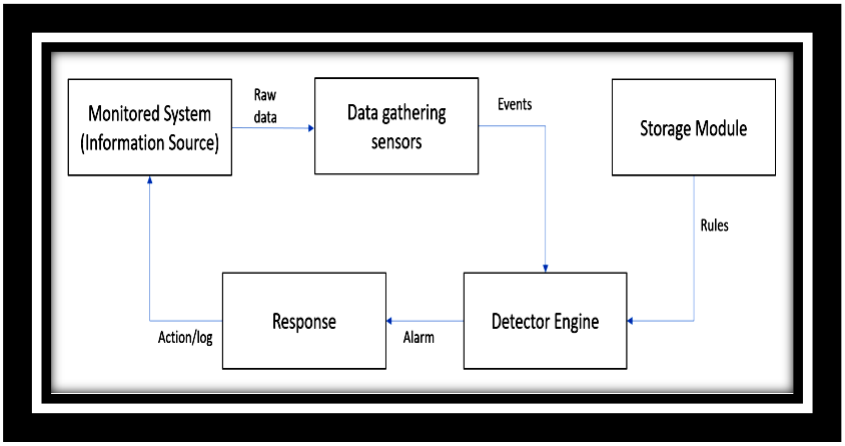

Figure 2 Intrusion Detection System architecture

II. LITERATURE REVIEW

Ali Hameed and others The Internet of Things (IoT) is a phenomenon that is pervasive in modern society. Using this technology can be advantageous for cities, hospitals, and homes in a variety of ways. A network of connected objects known as the Internet of Things (IoT) broadcasts and receives a variety of data. The attacker's desire for valuable data allowed for an attack on the IoT networks. Due to their poor performance, current security techniques must be modified in order to safeguard IoT devices. Lightweight algorithms must be offered to support IoT devices in order to get around this limitation. In order to defend against a variety of assaults while taking into consideration the system's limits, many algorithms and authentication techniques for the Internet of Things (IoT) were examined in this paper[12].

Ashwini B. Abhale and others Over the past ten years, internet usage and growth have continuously increased. Similar to this, a variety of new services have been introduced on the internet to offer conveniences to people. Fire safety, military use, monitoring of the oil sector, security system monitoring, and environmental monitoring are just a few of the many uses for wireless sensors. Because of their low battery life, limited bandwidth, dispersed architecture, and self-organization, nodes in WSNs are susceptible to a number of security-related attacks. The OSI model's layers are all susceptible to WSN attacks. As a result, wireless sensor nodes have a range of problems, such as functional problems and attacks-related defects. For the purpose of identifying and preventing attacks, it is crucial to install defences and network monitoring tools. The duty of an IDSS requires both issuing an attack alert and detecting internal threads (IDS). In this study's intrusion detection system, intrusions are found using supervised classification models like the Random Forest classifier, SVMs, Decision Tree classifier, LGBM classifier Extra Tree classifier, Gradient boosting classifier Ada boost classifier K Nearest Neighbor classifier, MLP classifier, Gaussian Naive Bayes classification, and Logistic Regression classification. Based on a modified version of the KDD99 data set, this dataset was created. The support vector machine exhibits the highest accuracy in the experiments when compared to a few other categorization systems[13].

Arjun Shakdher and others Through rigorous penetration testing, flaws in IoT apps were found. A series of man-in-the-middle attacks that took use of the most prevalent OWASP-defined security issues were also conducted as part of this research. Over a million users have downloaded a number of IoT apps, including those for linked cars, smart homes, security systems, and healthcare, that have been proven to be open to various types of assaults. Several solutions were suggested[14] in order to guarantee the security of IoT apps.

Abinaya.E. and others The Internet of Things makes connectivity and networking possible at any time and from anywhere (IoT). Our lives will be made simpler by the Internet of Things because it will enable our digital environment to be sensitive, adaptive, and responsive to our requirements. The main cause of network security flaws is attacks on software systems. Buffer overflows are a technique used by viruses, Trojan horses, worms, and denial-of-service attacks to introduce harmful code into the system. The assault will be thwarted by the usage of cryptographic algorithms like Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). These algorithms are implemented using Cryptool, and the effectiveness of loT devices is evaluated[15].

The CC environment can be protected from a variety of security threats using a number of methods [16]. In [17], the authors developed a technique based on Support Vector Machines (SVM) to secure cloud computing while minimising the over-fitting issue. However, over-fitting the model selection criterion might have a significant impact on the kernel models. To create the security model, an Artificial Neural Network (ANN)-based technique has been suggested in [14]. Although ANN has a great capacity for parallel processing and can store data over the whole network, its performance depends on the hardware since parallel processing requires powerful processors. In [17], the authors suggested a decision tree-based method for detecting network anomalies. Additionally, [16] proposes a hybrid machine learning model. This method combines the benefits of two learning approaches, but it also makes the system more complex. To identify network threats, the authors of proposed a Bayesian network-based model in [17]. However, due to sigma functions and cross-corpus calculations, Bayesian networks require a significant amount of computer power.

MukrimahNawir and others A network of interconnected smart devices that frequently exchange data over the Internet is known as the Internet of Things (IoT). IoT security is essential because it could contain sensitive data and safety-critical operations. IoT is a new technological paradigm. In the smart home, healthcare, and transportation industries, network security concerns are the main topic of this article. It's possible that an interruption in the operation of IoT devices will cause them to enter shutdown mode. We've

developed a taxonomy of IoT security attacks[18] to assist IoT developers in better comprehending the risks posed by security issues and how to implement stronger defences.

III. CLOUD COMPUTING CHALLENGES AND SECURITY RISKS

The following is a list of attacks and threats to cloud security:

Hijacking of accounts and services is one of the most serious security risks. This occurs when hackers attempt to compromise a web service on a website that is hosted by a cloud server or service provider, after which they install their control software on the cloud provider's infrastructure [19].

Abuse and nefarious use of cloud computing: For this kind of assault, the attacker can exploit the cloud infrastructure's computational capacity to attack targets with spam and malware like botnet. It is the biggest security risk in cloud computing, according to the CSA. Attacks using the backdoor channel: This type of attack occurs when an effective user has a high level of permeation at the VM or Hypervisor level. Data privacy and service availability may be impacted by this.

Cross site scripting attacks: XSS is another name for it. One of the strongest attacks on security flaws discovered in online applications. The Java script language is one of the most versatile scripting and is frequently used in such attacks.

Cloud malware injection attack: One of the top security lists for cloud computing, this attachment's goal is to introduce malware, a malformed application, or a virtual machine into the cloud architecture.

Denial of Service attacks: When users intend to request the service from the server under this kind of attack, it won't be there. They will experience the service is not found error 404.

Insecure application programming interface: This type occurs when service providers use APIs to deliver their services to clients, and those APIs include mechanisms for secure access control, secure authentication, activity monitoring, and encryption.

Man in the middle attacks: In this kind of attack, the hacker establishes an independent link between the user and the service provider to secretly view the data and information for the service.

Metadata spoofing attack: In this type, the web service providers transmit the client system the service metadata document, which contains all the details about the service invocation, including the message format, network location, and security specifications. In this instance, the attacker wants to change the network endpoints and references to the security policies in order to reengineer the web service metadata descriptions.

Malicious insiders: This type of security risk arises when there is a lack of security consideration for how employees can access the service provider to the cloud's virtual properties. Due to employee privileges not being implemented in the cloud system and outdated duties when their behaviour or position changed, this threat may be more complex.

Phishing attack: By enabling users to access phoney web links installed on their PCs, malicious software expose that data, compromising user privacy and exposing their data and information.

SQL Injection attacks: This type of problem occurs when hackers attempt to access a website's database by inserting malicious code into SQL statements and employing website query techniques to disable a security feature.

Shared technology's vulnerabilities: This problem was related to cloud computing, which makes use of internet infrastructure that is shared by all cloud users. As a result, every issue currently plaguing internet infrastructures will be moved to the cloud. The traditional parts, on the other hand, have not been designed to share the resources in cloud computing systems.

Sniffer attacks: This issue was associated with cloud computing, which makes use of shared internet infrastructure for all users. Every problem currently affecting internet infrastructures will consequently be transferred to the cloud. On the other hand, conventional components have not been created to share the resources in cloud computing systems.

Unknown risk profile: This kind of security risk arises as a result of focusing solely on the benefits and functionality acquired by using cloud services, without taking into account the security technologies and manufacturers that will be created. The issue is which features might obtain data from third parties and that data might then be shared for a variety of reasons.

Zombie attack (DoS/DDoS): It occurs when a host is directly or indirectly flooded at the Hypervisor, Network, or VM level. It can impact the availability of the service and create a user account for erroneous service usage.

IV. TYPES OF CLOUD

The architecture of cloud computing is diverse; the client is free to select any of them based on the required hardware, software, and price. In essence, cloud architecture looks like this [19].

Public Cloud: This particular cloud computing architecture was created with the client's usage plan model payment in mind. Microsoft Azure, Google App Engine, and Amazon Web Services are a few examples of this kind.

Private Cloud: This kind of cloud computing architecture is designed for use by commercial businesses and organisations as well as vital infrastructure. Public use of this type of cloud computing environment is not permitted. Government data centres and private company data centres are examples of private clouds.

Community Cloud: A variety of different stakeholders are involved in this robust infrastructure, which enables the third party to offer applications and platforms on which new services can be established.

Hybrid Cloud: Public and private clouds are combined in this form of cloud computing architecture. It is described as "a hybrid cloud that has a combination of public and private clouds connected together by either standardised or proprietary technology that facilitates data and application portability" by the National Institute of Standards and Technology (NIST).

Utility computing, another name for cloud computing, has seen a sharp increase in the number of service providers. These service providers provide elastic and flexible cloud computing services, such as virtual servers and storage, based on an on-demand paradigm, making it possible for numerous clients and organisations to do so [20].

V. CONCLUSION AND FUTURE WORK

Recent years have seen a significant increase in interest in academic and industrial disciplines for cloud computing, which is seen as the foundation of contemporary societies. Costs are cut and economic efficiency are increased by cloud computing. Governments, organisations, and businesspeople are searching for cloud computing's enabling features. The adoption of cloud

computing is still a ways off in the near future, though, because there are still a lot of security and privacy issues that need to be resolved. The most recent hazards and difficulties associated with cloud computing have been recognised in this paper. Our upcoming study will focus on developing a security model that takes the dangers and difficulties outlined into account.

REFERENCES

[1] V. B. Reddy, A. Negi, S. Venkataraman, and V. Raghu Venkataraman, "A Similarity based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT)," IEEE 5th World Forum Internet Things, WF-IoT 2019 - Conf. Proc., pp. 278–282, 2019, doi: 10.1109/WF-IoT.2019.8767170.

[2] Z. Chkirbene, S. Foufou, M. Hamdi, and R. Hamila, "Scalnet: A novel network architecture for data centers," in 2015 IEEE Globecom Workshops (GC Wkshps), Dec 2015, pp. 1–6.

[3] Z. Chkirbene, S. Foufou, and R. Hamila, "Vaconet: Variable and connected architecture for data center networks," in 2016 IEEE Wireless Communications and Networking Conference, April 2016, pp. 1–6.

[4] Zina Chkirbene, Ala Gouissem, Rachid Hadjidj, Sebti Foufou, and Ridha Hamila, "Efficient techniques for energy saving in data center networks," Computer Communications, vol. 129, pp. 111 – 124, 2018.

[5] Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp. 200 – 222, 2016.

[6] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, no. Icoei, pp. 1019–1024, 2019, doi: 10.1109/ICOEI.2019.8862720.

[7] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, ``Cybersecurity for industrial control systems: A survey," Comput. Secur., vol. 89, Feb. 2020, Art. no. 101677.

[8] A. Hijazi and J.-M. Flaus, ``A deep learning approach for intrusion detection system in industry network," Tech. Rep., 2019.

[9] I. E. Mir, D. S. Kim, and A. Haqiq, ``Security modeling and analysis of an intrusion tolerant cloud data center," in Proc. 3rd World Conf. Complex Syst. (WCCS), Nov. 2015, pp. 1-6.

[10] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustain. Cities Soc.*, vol. 61, p. 102343, 2020, doi: 10.1016/j.scs.2020.102343.

[11] N. Zhang, R. Wu, S. Yuan, C. Yuan, and D. Chen, "RAV: Relay Aided Vectorized Secure Transmission in Physical Layer Security for Internet of Things under Active Attacks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8496–8506, 2019, doi: 10.1109/JIOT.2019.2919743.

[12] A. Hameed and A. Alomary, "Security issues in IoT: A survey," 2019 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2019, pp. 1–5, 2019, doi: 10.1109/3ICT.2019.8910320.

[13] B. A. Ashwini and S. S. Manivannan, "Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network," Opt. Mem. Neural Networks (Information Opt., vol. 29, no. 3, pp. 244–256, 2020, doi: 10.3103/S1060992X20030029.

[14] A. Shakdhe, S. Agrawal, and B. Yang, "Security Vulnerabilities in Consumer IoT Applications," Proc. - 5th IEEE Int. Conf. Big Data Secur. Cloud, BigDataSecurity 2019, 5th IEEE Int. Conf. High Perform. Smart Comput. HPSC 2019 4th IEEE Int. Conf. Intell. Data Secur., pp. 1–6, 2019, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00012.

[15] E. Abinaya, K. Aishwarva, C. P. M. Lordwin, G. Kamatchi, and I. Malarvizhi, "A Performance Aware Security Framework to Avoid Software Attacks on Internet of Things (IoT) Based Patient Monitoring System," Proc. 2018 Int. Conf. Curr. Trends Towar. Converging Technol. ICCTCT 2018, pp. 1–6, 2018, doi: 10.1109/ICCTCT.2018.8550955.

[16] Zina Chkirbene, Aiman Erbad and Ridha Hamila "A Combined Decision for Secure Cloud Computing Based on Machine Learning and Past Information" 2019 IEEE Wireless Communications and Networking Conference (WCNC), 978-1-5386-7646-2/19 ©2019 IEEE.

[17] Laura Auria and Rouslan A. Moro, "Support vector machines (svm) as a technique for solvency analysis," vol. 1, 02 2008.

[18] M. Nawir, A. Amir, N. Yaakob, O. B. Lynn, and C. Engineering, "2014 2nd International Conference on Electronic Design, ICED 2014," *2014 2nd Int. Conf. Electron. Des. ICED 2014*, p. 542p, 2011.

[19] SUBBIAH, M., D.S.S. MUTHUKUMARAN, and D. RAMKUMAR, Enhanced Survey and Proposal to secure the data in Cloud Computing Environment. International Journal of Engineering Science, (2013) 5.

[20] Hussam S. Alhadawi Mohammed Hasan Ali, Laith M. Kadhum , Mohamad Fadli Zolkipli "A Review of Challenges and Security Risks of Cloud Computing" Journal of Telecommunication, Electronic and Computer Engineering e-ISSN: 2289-8131 Vol. 9 No. 1-2.