Cloud Security: Challenges, Attacks, and Techniques

John Hanley, Md Minhaz Chowdhury and Mike Jochen

Computer Science Department

East Stroudsburg University

East Stroudsburg, PA 1830

Jhanley5@live.esu.edu, Mchowdhur1@esu.edu, Mjochen@esu.edu

Krishna Kambhampaty

Computer Science Department

North Dakota State University

Fargo, ND 58102

K.kambhampaty@ndsu.edu

Abstract

The realm of cloud computing is steadily progressing, increasing the number of consumers adopting the service. This realm has become a larger target for many individuals with the technical ability and malicious intent to execute assaults upon. That is why cloud security has become such a prevalent topic for conversation in today's technology dependent society. While there exist many vectors for attack on cloud based systems, this paper aims to examine only a select few that are commonly recognized such as data breaches, denial of service attacks and those of similar nature. In addition, the goal is to also analyze and explore some of the current mitigations being utilized and put in place, such as encryption, intrusion detection systems, and firewalls. This also includes possible advancements that have tried making innovations within this area of study. The paper concludes that, cloud security must deal with the many issues that trouble cloud computing before the potential of the cloud can be attained and prove beneficial.

1 Introduction

Cloud security has risen as an important topic of discussion within the field of technology. It is the protection of cloud-based data, applications, and infrastructures, ensuring their confidentiality, integrity, and availability while checking for appropriate authentication and authorization. Unfortunately, there is no such thing as being one hundred percent secure. While cloud security is not altogether insecure, there are many issues that instill hesitation within those who would consider using and adopting the cloud. Some include data theft, data leakage, and availability of services. This sense of worry in people is what cloud security hopes to ease.

Cloud security is crucial for both consumers and producers who are concerned with the protection of computing resources based in the cloud. It is relevant to any members of the public who use services provided by companies, such as Apple, Google, and popular social media applications, that use the cloud to store data. This also pertains to small and medium sized businesses who have most of their organization based on the cloud, relying on the services provided by companies like Microsoft and Amazon. In the event that any of these services provided end up exploited or infiltrated, attackers can do whatever they desire with the information and data to which they have gained access. This can range anywhere from personal consumer information to credit card data and items of a similar nature. In terms of the impact it would have on businesses, attackers could cost them millions of dollars and even gain access to vital intelligence that has the power to destroy the company's livelihood. As the world gradually becomes dependent upon the cloud, it is imperative that individual users and businesses become aware of the countermeasures their chosen cloud provider has in place for them. This will provide consumers insight into how secure their information is being kept. The crucial role that security plays within the cloud is why this composition hopes to explore the current state of cloud security.

The aim of this paper is to explore and analyze the types of challenges and attacks the cloud faces, as well as possible solutions that could be of use. Typical methods used by attackers include XML wrapping attacks, denial of service attacks, and types that focus on damaging, as well as inhibiting, services performed by virtual machines. To try and stop hostiles, security experts utilize various mitigation techniques such as encryption, host/network IDSs, and access controls. However, while it is the duty of the cloud service provider to ensure the overall safety of a client's resources, most of the responsibility for securing the workload lies with the customer. It is their duty to ensure that all individuals using the cloud on their end are trained to handle the resources correctly. That means making them aware of proper security habits and procedures as well as any dangers that can impact the cloud. As with any field, research is being performed in search of possible advancements that could be of benefit to cloud security. This includes technologies such as blockchaining and VMI. Blockchain technology has gathered

attention as a result of being able to provide every user on a network with a shared, fault-tolerant database and thus the ability to nullify malicious users [1]. Likewise, VMI technology is popular in the cyber security field [2]. Cloud security must address and resolve many issues, before cloud computing can exist as the next generation provider of society's data storage and computing resource needs.

The rest of this paper is organized as follows: section 2 shall discuss prevalent background knowledge to assist in providing a better understanding about various aspects of cloud security. Section 3 analyzes the problems that cloud services face. Section 4 discusses common attacks inflicted upon the cloud. Section 5 covers some possible mitigation techniques. Section 6 concludes the paper, summarizing key points and ideas made throughout the material.

2 Background

The realm of cloud is exposed to numerous security threats. Everyday new threat emerges. The threat ranges from hackers to cloud service providers' deception. For example, cloud service provider can deceive the consumer for financial gain [3-6]. Remedy of such threats is patching up the vulnerabilities of the cloud computing life cycle. Remedies include, but not limited to, the applications of machine learning, data mining, artificial immune system etc. Machine learning is a set of scientific methodologies that learns from the problem environment it need to solve [7, 8]. Again, data mining is the extraction of interesting information from a large collection of data [9, 10]. Artificial immune system simulates the mammals' immune system to solve a given problem [11]. Before jumping into such mitigation techniques dealing the cloud security issues, cloud security concept need to be realized.

To better understand cloud security, one must have some basic knowledge about the cloud. According to [12], cloud computing is recognized as a model that allows for the constant, tailored, and opportune access to a collection of computing resources, over the internet. This hive of assets is shared amongst various customers, meaning their allocation and distribution is quick, requiring little to no intervention by providers. The cloud is a rather young technology that is still in its early stages, rising in its adoption throughout the world by businesses, governments, and individuals. The security concerns aside; the cloud has various properties that make it rather convenient to utilize.

One of the main components of the cloud is virtualization, which is in essence the making of a resource, like an operating system, virtual. The main purpose for this technology is to help streamline workloads by making computing more efficient and utilize resources to their full capabilities. Another important feature is that of multi-tenancy, where cloud

services allow consumers to share resources concurrently. Each “tenant” or user, has their own data isolated and hidden from others. Think of it in terms of the various apartments within an apartment building, thus the term “tenancy”.

The cloud is said to have five main properties, the most prevalent being: [12]

1. On-demand self-service: If a specific consumer demands the service provider promised resource, then the resource is provided to that consumer.

2. Broad network access means that resources and services are accessible across a vast number of devices and distances due to using the internet.

3. Rapid elasticity refers to the ability to quickly adapt the amount of resources allocated in order to suit the intensity of a workload.

These properties are applied to the four models through which services are deployed.

The private cloud model issues resources to one organization and any sub-units within it. This cloud is geared towards businesses [12]. The community cloud is similar to the private in that it primarily caters to companies. However, rather than being issued to a single organization, it is provided for a group or community of businesses that share similar resource requirements and needs [12]. The public model has resources sectioned off for open utilization by the masses in the style of a business to consumer transaction [12]. The last version is the hybrid, which is a combination of the private and public clouds. It keeps the two separated, but connected, through the process of sharing data and applications between each other [12]. These models are used to provide the cloud’s three main services.

The first service, Infrastructure as a Service (IaaS), gives consumers the ability to acquire a computing infrastructure and all the necessary components necessary to utilize it. Clients have no control over the actual infrastructure, but can manage operating systems, storage, applications and more [12]. An example of this form of service would be something akin to Amazon Web Services (AWS). Platform as a Service (PaaS) comes with an environment for its consumers where developers can create and work on various projects. The patron only has control over the released application(s) and perhaps settings of the environment that is hosting the service [12]. An instance of this type would be Windows Azure. The last one is Software as a Service (SaaS), offers services hosted on the cloud. The consumers can access such service through the API (Application Programming Interface). This sort is often based on a subscription that is charged on a monthly basis [12]. A well-known representation of this would be Office 365.

Now that the general basics of the cloud have been covered, some insight behind security methods and techniques may assist in comprehending ideas discussed later. A common security tool is an intrusion detection system, or IDS, which analyzes and keeps an eye on traffic moving across a network, or host, in order to spot odd or suspicious activity. There are many different versions and it is commonly used in some combination with an IPS, or

intrusion prevention system. An IPS is similar to an IDS, but rather than just alert a system to suspicious behavior, it is also able to take action upon strange activity.

A rather new technology, blockchaining has gained popularity due to its use in virtual currency such as BitCoin. Blockchaining has only recently been proposed for use within cloud security. It acts as a shared public record or database, where a single exchange is noticed and acknowledged by all nodes within the network, each has its own version of the record updated to reflect any changes that were made [1]. While not new to computer security, virtual machine introspection (VMI) is still new in how it is utilized within the cloud. VMI acts as a means to observe and gather information about a virtual machine's current state, detecting if there are any changes or movement [13]. This is used on the virtual machine monitor (VMM) or hypervisor.

Hypervisors are broken into two categories and the version that cloud providers usually use are type 1 hypervisors. This is software, firmware, or a mixture of the two, that performs the duty of coordinating physical hardware resources to virtual machines. These are installed onto hardware and intended for server sized systems, since they require a lot of power. Having covered all the background information needed to understand the topics of discussion, the paper shall proceed with its analysis.

3 Challenges of securing the cloud

Each of the three main cloud service models have security issues and needs that are unique to them. The responsibility to oversee these problems belongs to the cloud service provider, customer, or both. This makes it challenging because it requires having different security frameworks in place for each model. As opposed to having a single universal frame that can be applied and tailored to all. However, it makes it more tasking for the attacker, since it means that they have to understand more about the various security layouts. Rather than being able to exploit one model and then apply that same process to the others.

The IaaS model has security issues primarily aimed at its use of virtualization. Securing the hypervisor is the duty of the cloud service provider. According to [14], "Any compromise of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted". This would allow attackers the ability to see private operations of VMs, belonging to various clients, in plaintext or at least in some understandable form. Thus, providing them with more information that could assist in future assaults, or even worse, they could gain control of a hypervisor and everything in its scope should they compromise it. Another matter of security that is overseen by cloud providers is protecting any virtual networks that are being distributed to clients. As with

other resources, network infrastructures are split across various users. [14] states that by doing this split, the cloud "… will increase the possibility to exploit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities, or even the vSwitch software". This can lead to various network based attacks such as IP spoofing and DNS hijacking, all of which could allow attackers the opportunity to expand their vectors for attack and increase their chances of success.

The PaaS model uses Service-oriented Architecture (SOA) as a basis for its functionality [14]. In essence, cloud providers and their customers collaboratively focus on security matters pertaining to providing services through the internet. As a result, risks include common web attacks such as barrages of DoS, Man-in-the-middle attacks, and various injections. PaaS also has a need for security to be put in place to guard the APIs it provides. APIs, application programming interfaces, are collections of resources used to assist in the creation of and communication between software. Establishing mutual authentication, authorization and web service security standards between providers and customers is important to securing cloud services [14]. These actions are necessary in order to prevent any unauthenticated and unauthorized calls to said APIs, by attackers who hope to gain access to information not intended for them. For example, stopping them from being able to acquire personal content stored on a database, that communicates with an insecure API lacking the proper authentication measures.

The SaaS model has to deal with a combination of data and network security issues, but it focuses most of its efforts on the protection of web applications hosted through the cloud. In [14], it is stated that "web application security misconfiguration or weaknesses in application-specific security controls is an important issue in SaaS". Like PaaS, much of the responsibility for security is placed upon the joint efforts of cloud service providers and their clients. Therefore, it is necessary to review each application for any flaws in their controls. This is to ensure that the multiple users who may have their own security setup, do not cause conflicts in a way that create holes or vulnerabilities in the system's security configuration. There are many different ways in which the cloud can be attacked, as it is exposed to the threats of the internet.

4 Common Attacks in Cloud

First, there are two types of attackers that can inflict damage to the cloud, external and internal. The external attacker exists outside of the cloud and has seen a rise in numbers. They are often focused on affecting the cloud's availability, an extremely important aspect [15]. The internal attacker is already within or apart of the cloud system. This attacker has much more knowledge about the inner workings of the system and how security may be laid out, making it less difficult for them to penetrate defenses [15].

Typical attacks leveraged upon and within the cloud include different types of DoS, VM oriented assaults, and web attacks. The types of DoS that impact VMs are guest and VMM. A guest DoS is when a single VM on the system is able to use up all resources due to a leveraged vulnerability in a hypervisor or an incorrect configuration [2]. Preventing other machines from being able to perform properly. A VMM DoS is aimed at the system's virtual machine monitor. This is when resources such as RAM, CPU, and bandwidth are withheld, negatively impacting the performance of various operations and VMs [2]. The cloud is vulnerable to the typical forms of DoS that threaten networks, often used in conjunction with flooding and IP spoofing techniques.

When dealing with VMs, attackers target the lowest level of the system architecture, attempting to gain more control and widening their options for attack. There is also the added benefit of being able to hide their tracks and presence better. A VMM hyperjacking is when a deceptive hypervisor is installed that is capable of taking over the reins of a server or the like [2]. For example, rootkits are quite feasible to be the cause of such an attack. With VM escape, the security of virtual boundaries becomes a serious problem. This is when an attacker gains access to memory and resources beyond the domain of the infiltrated VM, having the ability to read, write or execute the contents [2]. They would have access to multiple resources belonging to the same company or multiple companies, from there possibly being able to connect to other VMs on a different server and growing their access.

This leads to a large fear for many cloud consumers which is a data breach. A data breach occurs when individual(s) or organization(s) gain unauthorized access to what one may consider confidential information [16]. Incidents of this type are often treated as far more severe in the cloud than elsewhere since providers are not necessarily storing just one company's data but a variety of business' data [16]. Therefore, should an attacker successfully breach data belonging to a particular company, they could potentially continue to breach the data of other business's located on the same server. This is one of the reasons why the cloud is such a perfect target for attackers who desire to compromise and expose data.

The cloud's heavy amount of interaction with the internet makes Web attacks an issue of concern. Injections such as SQL injection are common attacks. It is the insertion of a manipulated SQL query that allows for the execution of commands on a database that provide access to confidential data [15]. Cross Site Scripting (XSS) is another form of attack used against web applications. XSS is the injection of malicious scripting code into an application sent to a web browser, where it is executed and sends any private information to the attacker [15]. This is because the end browser has no way of telling if the script is trustworthy, thus it assumes that since it came from a trusted source it is okay to execute. XML signature wrapping attacks have recently been used against providers like Amazon. These attacks are reliant on the cloud exchanging resources via the simple object access protocol (SOAP). Attackers fill the XML message structure with malicious content, it gets through security since the digital signature covers all elements, including the infected portions [17]. As there is a plethora of ways for the cloud to be attacked, there are also a number of ways to help combat them.

5 Security Techniques

In order to try and combat such problems, researchers have proposed a variety of innovative security countermeasures. Majority of cloud computing services are based on using internet as a medium to access the service, running the risk of exposing their contents. The offered services are accessible via APIs (Application Programming Interface), remote connections, virtual private networks, and file transfer protocols [14]. Controls are a security tool used to deter, prevent, and detect risks to a system. Therefore, it is very important for cloud providers to have a series of controls that are able to target vulnerabilities related to these various means of access. In order to protect any and all data exchanged between the cloud and its consumers. Cloud providers must also take care to ensure that they adhere to any compliance laws that pertain to data privacy and security in order to avoid any possible legal ramifications.

A common countermeasure that is often used is an IDS. An IDS is usually classified as being one of two types, host or network based. A host IDS (HIDS) focuses on the machine it is installed on, making sure that the traffic entering and leaving, as well as files on the system, are not behaving in a suspicious manner. A network IDS (NIDS) is similar to a HIDS, but focuses on a larger scale, looking at an entire network and analyzing all traffic for any malicious activity. “To protect a public or private cloud, an IDS which supports scalable and virtual environments is required” [18].

One of the proposed IDSs for the cloud is the Grid and Cloud Computing IDS (GCCIDS). It is intended to detect activity that has yet to be noticed by its predecessors. This is achieved by making use of deep learning technology. The GCCIDS is partially dependent on knowledge based analysis, which matches suspicious activity to any already known attacks recorded in its database [19]. Although this means that unknown attacks are unable to be detected, keeping the list of known attacks current can assist in lowering the risk of any hostile activity slipping through. It is also reliant on behavioral analysis, which is the aspect of the system that attempts to make use of deep learning technology to discover new forms of attacks and their patterns. According to [19], this functionality of the IDS “…uses feed forward artificial neural network (FFANN). However, FFANN is not useful at the starting phase due to little or no data availability”. This is often common with deep learning methods, the idea is that as time passes the system gains new data and information to build its knowledge, allowing it to start learning the difference between normal and abnormal activity. As the cloud becomes faster and larger, it will become too time consuming for individuals to continuously configure and monitor such tools properly. That is why I believe it is imperative to start finding ways to implement deep learning and artificial intelligence in a way that creates automated systems, whereby human interaction and involvement are lowered.

Another proposed security technique is the idea of a data provenance architecture based on blockchaining, called ProvChain. Data provenance in essence refers to the origination, tracking, and purpose behind a piece of data. [1] believes that by making use of blockchain's decentralized architecture, in which every node on the network assists in providing services, it can be leveraged to assure the security of data tasks. ProvChain claims to be able to monitor user actions in real time, provide an environment free from outside manipulation, have better privacy, and validate data. According to [1], this is achieved by using hooks and listeners to gather and record user activity, storing hashed provenance data as a block in the blockchain, hashing a user's ID while publishing data so both are unable to be determined, and using blockchain receipts containing information about a block and its transactions. Such a tool would provide an organized and clean manner for administrators to be able to trace and follow data back to its source in the event of an attack and other security violations.

There are also various virtual machine introspection frameworks that are trying to improve upon current VMI technology. [13] proposes T-VMI, a framework they claim guarantees integrity, privacy, and correctness. It ensures integrity and privacy by placing crucial code in a separate environment called the TrustZone [13]. The TrustZone is a hardware innovation that allows a core to create two environments, a trusted and untrusted, running them concurrently. It begins in the lower levels of the PC but can extend to higher ones as well. The trusted portion runs with least privilege, meaning resource access and use is based on minimal need. It is inaccessible by the untrusted portion unless the proper calls and exceptions are made. This attempts to protect from the manipulation of attackers who have corrupted a VM and try to report that the VM is still secure and running properly. T-VMI guarantees correctness by making use of the Secure Monitor Call (SMC). This escalates privilege level allowing the model to capture information about a VM, record the physical address of key data and access those addresses to make sure they are valid and true [13]. SMC attempts to protect against compromised hypervisors who have allowed attackers access and the ability to corrupt or falsify data and memory.

A firewall is very important as it assists in filtering out inappropriate traffic from that which is legitimate. They often perform at various levels of the system, coming in different types and are almost always apart of the first layer of defense. However, when it comes to the cloud environment they have proven themselves difficult to implement. According to [18], traditional packet level firewalls are unable to handle the various forms and amounts of traffic that travel through cloud networks. As a result, they have proposed a decentralized firewall that is able to perform various levels of security while averting malicious assaults, whether internal or external. The firewall appears to be intended to oversee a cluster of VMs within the cloud. [18] states that the firewall resources are distributed in a dynamic manner so that each cluster is able to establish their own firewall. The idea is that although separate, these firewalls will collaborate together to filter inbound traffic.

Implemented in most aspects of security, encryption is used to help maintain data and information confidentiality, integrity, and privacy. According to [20], encryption in the

cloud is performed at five different places: the user, application, middleware, database, and storage levels. Some encryption algorithms used in the cloud are AES, RSA, as well as Identity based (IBE) and Attribute based (ABE). Advanced Encryption Standard (AES) uses symmetric encryption, meaning that it requires only one key, a randomly generated value that is input into the algorithm to generate encoded data, for both encrypting and decrypting. It is faster and more secure than its predecessor, Data Encryption Standard (DES) [21]. AES encrypts and decrypts data in 128-bit blocks of data, capable of handling large amounts of information. One of its weaknesses is the matter of security when exchanging keys, since only one is used. This is resolved in RSA. RSA uses asymmetric encryption, meaning that it implements two keys, one public to everyone and one private, for encrypting and decrypting. As opposed to doing it in blocks, it handles the data all at once. Private key is used by the sender to encrypt the data. The encrypted data is then decrypted by the receiver using the public key. RSA is rather slow as it performs computations with very large numbers.

Less common, IBE is based on the idea that the public key is dependent upon the user's identity [21]. A Private Key Generator (PKG) creates the private key that corresponds to the public one, the receiver requests said key from the generator. This makes it possible to encrypt and decrypt messages without the need to send keys between the parties involved. ABE is dependent upon using a set of characteristics and roles associated with a user to generate the public encryption key [21]. The private key is generated based on a certain group of attributes. Whenever dealing with encryption it is of the utmost importance to make sure that key distribution and management takes the proper steps to ensure security and confidentiality.

6 Conclusion

Cloud security must deal with the many issues that plague cloud computing. This must be achieved before the cloud's potential can be fully realized and society as a whole can benefit from all it has to offer.

This paper viewed the various areas of focus specific to each cloud model and their respective weaknesses, including any necessary security needs. IaaS relies heavily on the use of virtualization. PaaS is exposed to the dangers of web attacks and internet related assaults. SaaS is vulnerable to the misconfiguration of controls and measures.

The composition takes a look at a series of common attacks performed such as DoS, assaults on virtualization components (VM hyperjacking), and XML wrapping. All these and more, cloud security has to find a way to mitigate so as to ensure and build trust in potential consumers who are still hesitant about utilizing the cloud.

It also explored various countermeasures that may be implemented in the cloud. These include IDSs such as the GCCIDS that uses deep learning technology. There was mention of securing the tracking of data by using blockchain technology, and the use of a VMI framework that can be trusted to report the true state of a VM. The paper covered different encryption algorithms used like AES, RSA, IBE, and ABE. In addition, it discussed a possible architecture for implementing a firewall inside the cloud that hopefully does not prove difficult to implement. The severity and consequences of the possible attacks discussed, goes to show how important of a role cloud security plays. If configured properly, cloud security can ensure data privacy and provide assurance to consumers that their information and services are being actively watched over. Cloud security holds the key to unlocking the cloud's potential.

References

[1] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, *The IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, Madrid, Spain, May 14-17, 2017.

[2] J. Zhang, L. Zheng, L. Gong, and Z. Gu, A Survey on Security of Cloud Environment: Threats, Solutions, and Innovation, *The Third International Conference on Data Science in Cyberspace*, Guangzhou, China, June 18-21, 2018.

[3] Md Minhaz Chowdhury and Kendall Nygard, Machine Learning within a Con Resistant Trust Model, *The 33rd International Conference on Computers and their Applications (CATA 2018),* Flamingo Hotel, Las Vegas, Nevada, USA, March 19-21, 2018.

[4] Md Minhaz Chowdhury, Kendall E. Nygard, Krishna Kambhampaty and Maryam Alruwaythi, Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm, *The 4th Annual Conference on Computational Science & Computational Intelligence*, Las Vegas, NV, USA, December, 2017.

[5] Md Minhaz Chowdhury and Kendall E. Nygard, An Empirical Study on Con Resistant Trust Algorithm for Cyberspace, *The 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing*, Athens, Greece, July 17-20, 2017.

[6] Md Minhaz Chowdhury and Kendall E. Nygard, Deception in Cyberspace: An Empirical Study on a Con Man Attack, *The 16th Annual IEEE International Conference on Electro Information Technology*, Lincoln, Nebraska, U.S.A, May 14-17, 2017.

[7] Rahul Gomes, Mostofa Ahsan and Anne Denton, Random Forest Classifier in SDN Framework for User-Based Indoor Localization, *The 2018 IEEE International Conference on Electro/Information Technology*, Rochester, Michigan, USA, 3-5 May 2018.

[8] Mostofa Ahsan, Rahul Gomes and Anne Denton, SMOTE Implementation on Phishing Data to Enhance Cybersecurity, *The 2018 IEEE International Conference on Electro/Information Technology*, Rochester, Michigan, USA, 3-5 May 2018.

[9] I. Jahan and S. Z. Sajal, Stock Price Prediction using Recurrent Neural Network (RNN) Algorithm on Time-Series Data, *The Midwest Instruction and Computing Symposium (MICS 2018)*, Duluth MN, USA, April 6-7, 2018.

[10] I. Jahan and S. Z. Sajal, Prediction on Oscar Winners Based on Twitter Sentiment Analysis Using R, *The 2018 SDSU Data Science Symposium*, Brookings SD, USA, February 11-12, 2018.

[11] Md Minhaz Chowdhury, Jingpeng Tang and Kendall E. Nygard, An Artificial Immune System Heuristic in a Smart Grid, *The 28th International Conference on Computers and Their Applications*, Waikiki, Honolulu, Hawaii, USA, December 2013.

[12] P. M. Mell and T. Grance, SP 800-145. The NIST Definition of Cloud Computing, *National Institute of Standards & Technology*, Gaithersburg, MD, United States, 2011. [Online]. DOI: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[13] L. Jia, M. Zhu, and B. Tu, T-VMI: Trusted Virtual Machine Introspection in Cloud Environments, *The 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, Madrid, Spain, May 14-17, 2017.

[14] Mohamed Al Morsy, John Grundy, Ingo Müller, An Analysis of the Cloud Computing Security Problem, *The APSEC 2010 Cloud Workshop*, Sydney, Australia, November 30, 2010.

[15] H. Hammami, H. Brahmi, I. Brahmi, and S. B. Yahia, Security Issues in Cloud Computing and Associated Alleviation Approaches, *The 12th International Conference on Signal-Image Technology & Internet-Based Systems*, Naples, Italy, November 28 - December 1, 2016.

[16] N. C. Paxton, "Cloud Security: A Review of Current Issues and Proposed Solutions," *The Second International Conference on Collaboration and Internet Computing*, Pittsburgh, Pennsylvania, USA, November 1-3, 2016.

[17] A. Alshammari, S. Alhaidari, A. Alharbi, and M. Zohdy, Security Threats and Challenges in Cloud Computing, *The 4th International Conference on Cyber Security and Cloud Computing*, New York City, New York, USA, June 26-28, 2017.

[18] C. Saadi and H. Chaoui, A new approach to mitigate security threats in cloud environment, *The Second International Conference on Internet of things, Data and Cloud Computing,* Cambridge, United Kingdom, March 22-23, 2017.

[19] M. Azeem, I. M. Khalil, and A. Khreishah, Cloud Computing Security: A Survey, *Computers*, Volume 3, Issue no 1, February, 2014.

[20] A. Saxena, V. Kaulgud, and V. Sharma, Application Layer Encryption for Cloud, *The 2015 Asia-Pacific Software Engineering Conference*, 2015.

[21] S. D. Choubey and M. K. Namdeo, Study of data security and privacy preserving solutions in cloud computing, *The 2015 International Conference on Green Computing and Internet of Things*, 2015.