Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)
© 2021 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/APC210188

MISP: Model for IaaS Security and Privacy

INDRA KUMAR SAHU [a,1], MANISHA J NENE [a]
[a] *Dept. of Computer Science & Engineering, Defence Institute of Advanced Technology, Pune, Maharashtra, India*

Abstract. Paradigm shift towards cloud computing offers plethora of advantages both for cloud users and Cloud Service Provider (CSP). For cloud users, it offers saving of cost, scaling of resources, pay per use, elastic and on-demand services. On the other hand, it offers centralized resource management and provisioning of operations, safety and security for CSP. By holding multiple virtual IT resources (CPUs, storage servers, network components and software) over the internet, Infrastructure-as-a-Service (IaaS) serves as fundamental layer for all other delivery models. Along with benefits of IaaS, there exists several security and privacy issues and threats to confidentiality, integrity, authentication, access control and availability. In this paper, detailed study of IaaS components, associated security and privacy issues are explored and counter measures for the same are determined. Furthermore, as a result of the study, Model for IaaS Security and Privacy (MISP) is proposed. The model presents a cubical structure and adds more features than the existing models to enhance the security and privacy of data and operations and guide security assessment for safer adoption by enterprises.

Keywords. Cloud Computing, Cloud Security, Cloud Deployment Models, Service Level Agreement, Model for IaaS Security and Privacy (MISP), IaaS, Virtualization

1. Introduction

Since the inception in late 1960s, cloud computing became a ubiquitous technology with hardware, software, computational and operational IT resources and services delivered via Internet to the users [1]. Elasticity, scalability, on-demand resources, cheap operational expenses, location and device independence and pay per use business model are the merits for its prime attraction [2]. Cloud computing has provided huge opportunity to migrate from maintaining, securing and operating own standalone, on-premise resources like infrastructure and applications to cloud. Recently, it attracted very considerable attention of academicians, industry people and researchers. As highlighted by NIST [7], cloud computing has three service models and four deployment models.

1.1 Service Models

IaaS with resources like data storage servers, computing hardware and networking components provides infrastructures to users to facilitate management of OS and applications.

[1] Indra Kumar Sahu, MTech scholar, Department of CSE,
Email: ikambition.s23@gmail.com.

Platform-as-a-Service (PaaS) where users are provided with an environment to develop, create and use their own tools and software applications.

Software-as-a-Service (SaaS) with readymade application software and tools are delivered to the users with licenses to use remotely without buying them completely.

1.2 Deployment Models

The deployment models define the way cloud may be used. The different models offer varying resources and the cloud users can adopt the one that suit them the best based on their needs and budgets. Four types of deployment models are as under.

Private cloud offers cloud resources and infrastructure to be used as stand-alone resources with greater control over security and data backup facility.

Public cloud offers shared resources at lower cost but the security and privacy of the data and storage lowered as compared to the private cloud.

Hybrid cloud shows the best of first two models in terms of resources, controls and the cost. The security and privacy are in between that of private and public cloud.

Community cloud offers shared resources amongst the same types of organizations like banks, hospitals etc.

1.3 IaaS Model

Cloud computing primarily depends upon IaaS delivery model that provides rudimentary operating systems, networking components, security infrastructure and data servers for designing and developing required applications, databases, development tools and services [8]. The Oracle and KPMG Cloud Threat Report 2020 [4] shows the recent adoption trends for cloud computing. As compared to 62% in 2018, in 2020 76% of on-premise business-critical applications migrated to IaaS through 'lift-and-shift' approach. Being the fastest growing sectors amongst all other service model, IaaS is expected to grow to $63 bn in 2021 from $ 23.6 bn in 2017 at a rate of 27.6 % according to Gartner [5]. It also predicted that by 2025, 80% of the enterprises will use IaaS as compared to 65% in 2017.

On demand services and scalable resources with advanced technical capabilities are provided to the users in IaaS model. Hardware comprising of storage servers, networking components and computing hardware (CPUs, RAM, graphic cards etc.) and software like cloud Application Program Interfaces (APIs), Utility Interfaces (UIs), hypervisors, software modules, security and control management modules are two types of components. Quality of Service (QoS) is an important factor and is made part of legal contract [5]. The IaaS model can also be viewed as shown in Figure 1 below [9].

From rigorous study on security and privacy issues of IaaS delivery, a Model for IaaS Security and Privacy (MISP) is proposed adding various IaaS components to mitigate the threats of the delivery model.

The rest of the paper is presented in four sections. Literature survey is in the second section. Third section is of preliminaries. The fourth section is for the proposed model MISP with details for enhancing the security and privacy in IaaS against existing vulnerabilities and threats. The fifth section concludes the paper along with future scope.

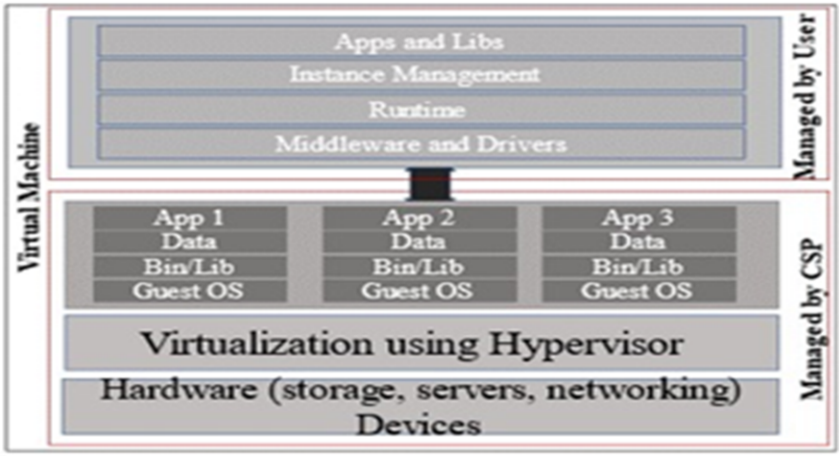

Figure 1. Virtual and Physical layer in IaaS [9]

2. Literature Survey

2.1 Related work

The security and privacy issues being faced in IaaS are related to Confidentiality, Integrity, Authentication, Availability and Access control (CIAAA) and a lot of research work has been done to mitigate these issues. Ravi et al. [10] carried out a sincere assessment of threats to security in IaaS along with responsibilities of cloud user and CSP. Their work mainly highlighted the issues in CIA triad and proposed possible solutions. The latest threats and focussed malicious approaches are not addressed.

Ahmed et al [9] presented brief of issues in IaaS components and analysed CSA top twelve threats in the model along with possible solutions for them. The threats mentioned in CSA report gets changed from time to time and hence are not very relevant at present time as per CSA report 2020 [4].

Cullum et al [35], in his paper presented host hypervisor security issues in public IaaS and their solutions. The detailed study on hypervisor gives out known attacks that exist in hypervisor shared environment. The solutions are focused mainly on virtualization related issues while other threats are not addressed.

Moutai et al [24], presented a secure architecture-based distributed testing to confirm CAA based on QoS. It is limited to information security. The parameters like security of storage, network and hardware are not tested.

Dawoud et al [8], presented IaaS security model with issues related to components, suggested secure policies along and restriction levels. The security model is limited to some issues only whereas, with the advancement in cyber spectrum, there is need of addition of latest issues and threats.

2.2. Contributions

Our paper presents a comprehensive cubical MISP that comprises of components related issues along with associated threats to IaaS model; each in the common plane of cloud user and CSP. There are rules and policies to enhance the security and privacy of data and operations in second plane. The third plane of cubical presents levels of rules and policies for implementation varying from lenient level to strictest level. The model summarizes all threats and possible ways out to enhance the security and guides security assessment for safer adoption of IaaS delivery model.

3. Preliminaries

3.1 Service level agreement (SLA)

SLA is a legal document agreed and signed between CSP and a cloud user to describe the legal responsibilities, liabilities for both of them and define QoS offered by the CSP as part of the agreement [12]. It makes a mention of both the required and the expected level of services to be delivered maintaining availability and security and privacy with review or monitoring of the SLAs, riders and liquidation terms and time span of contract.

3.2 Virtualization of Platform

Virtualization is a process of abstracting and sharing a single hardware that facilitates aggregating multiple stand-alone computing resources like CPUs, memory, storage and network components [8]. A typical example is 'Server virtualization' in which several attributes of physical server is hidden and they are reproduced in a hypervisor in the form of virtual CPU (vCPU), Virtual RAM (vRAM), virtual NIC (vNIC) and virtual disks. It has two important characteristics namely, multi-tenancy and scalability. The virtual and physical layers in the model are illustrated in figure 2 below.

Two types of virtualizations namely OS based in which a software is installed in host OS and hardware based that refers the installation directly on the physical host hardware [14].

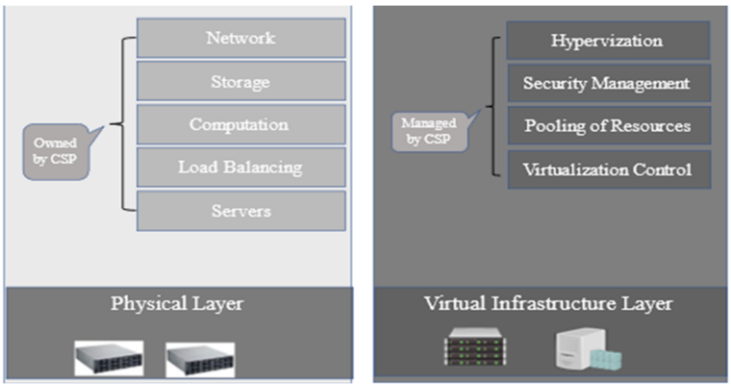

Figure 2. Virtual and Physical layers in IaaS

3.3 Utility Computing

Utility computing provides multiple resources on demand as per user's request. Various IT resources are packed for metered services and then provided to cloud users at low cost and as pay-per-usage basis with scalability support even if demand reaches to its peak [8].

3.4 Cloud Scalability

Cloud scalability being one of the basis of cloud computing, offers homogenous resources with infinite scalability at linear increase of performance; the answers to when, what and where to scale in multi-tier service-oriented applications in autonomic scaling [14].

4. Model for IaaS Security and Privacy (MISP)

Security of any service model in the cloud depends on the security of the infrastructure. Various components in IaaS are required to be looked into for user's satisfaction. Multiple agencies undertake works related to threat assessments on privacy and security on cloud computing. Distributed Management Task Force (DMTF), Open Cloud Consortium (OCC) and Cloud Security Alliance (CSA) are some of them that define standards, certifications and practices to ensure a secure cloud environment [18].

We propose a Model for IaaS Security and Privacy (MISP) in cubical form with three planes defined as shown in figure 3. The first plane gives out components of IaaS. The cloud user and CSP are common participants of the plane and they generally share responsibility in maintenance of security and privacy of the model.

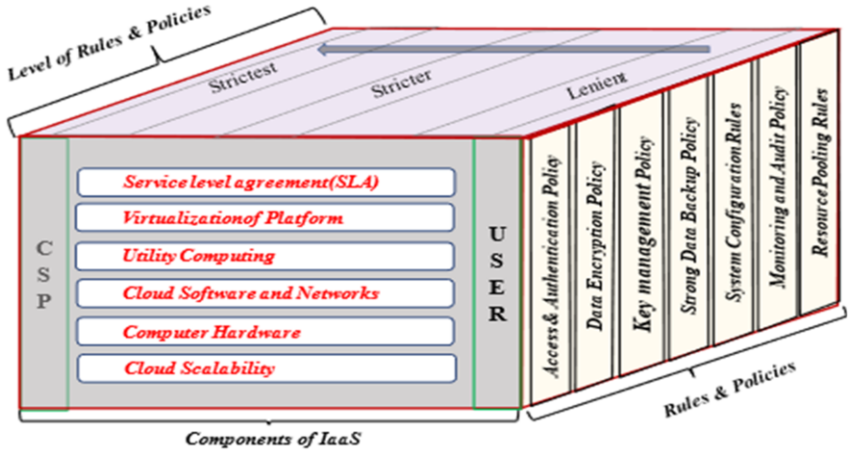

Figure 3. Model for IaaS Security and Privacy (MISP)

4.1 Threats Related to Components of IaaS

The plane consisting of components of IaaS in the proposed model is analyzed and threats associated with the solutions are described.

4.1.1 SLA Related Issues: Lack or non-existence of standardization in creating and performing the SLA between the involved parties creates big loopholes. The leading CSPs like Amazon (AWS), Google (GCP) and SalesForce hide numerous parameters regarding data safety and preservation in their proposed SLAs [6]. SLA may get exposed to vulnerabilities if any misunderstanding amongst the parties arises. So, it becomes imperative to detect user's concerns on priority [25]. The review and study of the environment displays several threats as per CSA classification.

Data breach and usage monitoring of data stored in the cloud is possible through human errors, application vulnerabilities, inadequate security practices or targeted attacks. Strong encryption techniques, prevention of leakage of secret data using neural networks [3], Data Leakage Prevention for Data in Transit using Artificial Intelligence and Encryption Techniques [34], strong backup and retention strategies and use of strong APIs [20] can mitigate this issue.

Insufficient due diligence while transferring responsibility of cloud control and cloud security to the CSP is a threat that is caused due to lack of transparency in security mechanism applied by CSPs [19]. Un-sanctioned application usage and sanctioned application misuse are the two key challenges in this threat. Strong key management [17], and use of SLA for cloud visibility are solutions for this issue.

Denial of Service (DoS) is a threat mainly due to external agents that can cause unavailability of resources to the cloud users in the form of network, application or bandwidth denial [18]. The threat can be mitigated with regular audits of log and monitoring of services with advanced methods like Software Defined Networks (SDN), EDoS and SEDoS [30].

Many of the researchers argue to propose Web Service Level Agreement (WSLA) that can manage SLAs in IaaS environment [36]. More conveniently, SLA monitoring and enforcement may be delegated to a third party to bridge the trust deficiency between the CSPs and the cloud users.

4.1.2. Virtualization Related Issues: Virtual-aware security is required to face the security issues in IaaS [15]. Three types of possible threats are determined here.

Threats from host Operating System*:* The host OS being privileged domain can monitor, configure, communicate and modify data or services and hence may cause threats to IaaS model. According to MacAfee Cloud Adoption and Risk Report [21], the average organization has 14 misconfigured IaaS instances at any given time making 2269 instances per month. 5.5% of AWS S3buckets in use are misconfigured. Strong data backup and retention techniques [22] and multi factor authentication can mitigate the threats.

Communication between host and the VM is through virtual network or shared virtual resources and hence vulnerable to threats. An attacker could exploit important features like Clipboard to monitor the activities between them [25]. In case of host being compromised, all the VMs get into risk of any kind of possible attacks. Trusted Virtual Domain (TVD) for infrastructure and security mechanism [29], Trusted Cloud Computing Platforms (TCCP) for confidentiality [31], VLAN for network virtualization and Identity Based Integrity Verification (IBIV) protocol for data integrity [13] are the solutions for such threats and issues.

Threats from VMs hosted on the same host: CSP provides API to carryout management functions such as provisioning, replication and decommissioning of resources on IaaS. But these insecure ill-designed, broken, exposed or hacked APIs and user interfaces (UIs) may lead to data breach or other security threats. Data Leakage

Prevention for Data in Transit using Artificial Intelligence and Encryption Techniques [34], Scarce Attack Datasets and Experimental Dataset Generation [27], multi-factor authentication and robust authentication mechanism [33] can mitigate these issues.

Other possible attack on virtualization platform is VM Escape in which isolation layer between host and VM is broken to get the access of hypervisor's root privileges. As the attacker gets control over the host OS, he can use the compromised OS to manipulate control as per his desires through covert channel for malicious code execution.

Network virtualization partitions or aggregates a collection of network resources and present them a unique and isolated physical view to the users. Communication between VMs is through network virtualization in a direct and efficient manner. To avoid attacks like sniffing, SQL injection and spoofing on virtual network, secure physical channels can be adopted.

4.1.3. Utility Computing Related Issues: The utility computing faces the challenge of complexity in cloud computing. A bigger CSP may lease the services to second level CSP who in turn provides metered service to users. For example, Amazon DevPay5 from Amazon is a second level CSP. In this, the second level CSP might use services and user may be charged for what he has not used. Strong multi-tier passwords and two-factor authentication mechanisms [23] maybe used to mitigate this issue.

4.1.4. Cloud Software and Network Related Issues: In IaaS model, CSP provides cloud software and networks. Open-source cloud software like Eucalyptus and commercially proprietary software are two options but security from vulnerabilities and bugs cannot be ensured in either of the two. Cloud providers either furnish APIs or web service protocols like XML Simple Object Access Protocol or simply SOAP to grant access to cloud users to orchestrate management functions.

4.1.5. Computing Hardware Related Issues: A pool of shared distributed physical resources is provided to cloud users through virtualization in IaaS. Threats and attacks in on-premises hardware scenario occurs internally as a study shows it to be 70% [16]. Threats can be categorized in various ways. Based on type of resources: threats to physical computing resources like CPU, monitor, other physical machines and threat to storage resources where attacker gets access of the data storage.

The other one is based on type of adversary: insider and outsider attackers. Insider attackers have access to the resources of the organization and can cause damage intentionally or otherwise [26]. The outsider may be any hacker or bot to damage the system. Policy Enforcement Points (PEPs) side caching [28], inclusion of human resource management are some of the mitigation techniques.

Management of various changes in internal, system practices and Identity and Access Management (IAM) affects identity, credentials, key and access management. Strong end to end encryption, multi-tier passwords and multi factor authentication, and LDPC decoders [11] are measures to mitigate it.

4.1.6. Cloud Scalability Related Issues: IaaS resources can be scaled as per the user requirements. While doing so, there is a threat of account hijacking and abuses to breach infrastructure through spam mails, social engineering, vishing and phishing. Strong encryption techniques, multi-factor authentication [23] for integrity and strict monitoring of unauthorized activities may help to tackle this issue.

4.2. Rules and Policies for IaaS

The rules and policies for security and privacy are presented in the second plane in a vertical axis that implicates their presence through all components of IaaS. They are as mentioned below.

1. *Access and Authentication Policy:* to restrict any unwanted and unwarranted users to get access and verify the authorized users of the IaaS delivery model.
2. *Data Encryption Policy*: to ensure confidentiality, integrity and authentication in IaaS model using strong encryption techniques.
3. *Key Management Policy:* to enforce no loss and misuse of keys used in the IaaS for various purposes.
4. *Strong Data Backup Policy:* to avoid loss, deletion, tampering or theft of data in event of any unprecedented natural disaster, data corruption or cyber-attack.
5. *System Configuration Rules:* to avoid system misconfiguration, system bugs and internal or external attacks through exploitation.
6. *Monitoring and Auditing Policy*: to prevent any intrusion, system failure, status of software, untoward event and possible security breaches.
7. *Resource Pooling Rules:* To utilize the resources available with CSP for users as per demand optimally and judiciously.

4.3 Levels of Rules and Policies

The third plane is level of rules and policies. The level of rules and policies implementation need to be based on judicious scrutiny of security of data and operation on IaaS infrastructure, expertise of the user and the environment. If the data and operation are of critical in nature, the strictest level to be followed. In case of normal or low value data and operations, lenient level may be implemented. Since the strictest level might be slow and time consuming, the levels may be decided accordingly.

The proposed model is an attempt to standardise the IaaS layers, various components present in the model that are threatened and rules and policies to mitigate the threats, issues and challenges. Level of rules and policies implementation suggest degree to enhance the privacy and security accurately traded off between operational time and required security.

5. Conclusion and Future Scope

IaaS delivery model provides the basis for all other models and faces the security issues across hardware and software. Virtualization is core of the IaaS model for isolation. The security and privacy issues arise due to numerous reasons like lack of adequate knowledge, complex policies, technical glitches, system errors, standardization, certification and violation of established policies and practices. In this paper, security issues associated with IaaS components are investigated. The security issues related to security of each IaaS components and proposed countermeasures are provided. The proposed MISP summarises all the issues and possible ways out to secure IaaS model to enhance the security and guide security assessment for safer adoption by enterprises. Cryptography and the best available techniques-based solutions are proposed to mitigate the threats to manage and secure the cloud in an optimal manner

Due to phenomenal rise in computing capabilities, the existing issues and challenges may get aggravated to unimaginable level of difficulties. New technologies like Network as a service (NaaS), Cloud of Things (CoT) etc. may pose different challenges. Timely review of the issues with the changes in policies and procedures will be warranted.

Another imminent threat is from quantum computing that possess extremely high computing capabilities. So, the security and privacy concerns of IaaS are required to be seen in the prism of quantum threats. The future work may be carried out to find quantum solutions in cloud computing for the post quantum era.

References

[1] Madni, S. H. H., Abd Latiff, M. S., & Coulibaly, Y. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities. Journal of Network and Computer Applications, 68, 173-200.

[2] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[3] Ghouse, M., & Nene, M. J. (2020, June). Graph Neural Networks for Prevention of Leakage of Secret Data. In 2020 5th International Conference on Communication and Electronics Systems (ICCES) (pp. 994-999). IEEE.

[4] Oracle and KPMG "Cloud Threat Report 2020", https://www.oracle.com/in/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf, assessed on 17 Dec 2020.

[5] Gartner, Infrastructure-as-a-Service Adoption and Risk Report. [Online] Available:https://www.gartner.com/en/newsroom/press-releases, accessed on 20 Mar 2021.

[6] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at dif ferent layers of Cloud computing, 1-32.

[7] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[8] Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In 2010 the 7th International Conference on Informatics and Systems (INFOS) (pp. 1-8). IEEE.

[9] Ahmed, A., & Zakariae, T. (2018). IaaS cloud model security issues on behalf cloud provider and user security behaviors. *Procedia computer science*, *134*, 328-333.

[10] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

[11] Rao, R. G., & Nene, M. J. (2019, March). CNR: A Technique for Data Replication Organization in BigData. In 2019 IEEE 5th International Conference for Convergence in Technology (I2CT) (pp. 1-6). IEEE.

[12] Remesh Babu, K. R., & Samuel, P. (2019). Service-level agreement–aware scheduling and load balancing of tasks in cloud. Software: Practice and Experience, 49(6), 995-1012.

[13] Sahu, I. K., & Nene, M. J. (2021, February). Identity-Based Integrity Verification (IBIV) Protocol for Cloud Data Storage. In 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-6). IEEE.

[14] Lloyd, W., Pallickara, S., David, O., Arabi, M., & Rojas, K. (2014, March). Dynamic scaling for service oriented applications: implications of virtual machine placement on IaaS clouds. In 2014 IEEE International Conference on Cloud Engineering (pp. 271-276). IEEE.

[15] Amato, F., Moscato, F., Moscato, V., & Colace, F. (2018). Improving security in cloud by formal modeling of IaaS resources. Future Generation Computer Systems, 87, 754-764.

[16] Markatos, E. (2008). Large Scale Attacks on the Internet Lessons learned from the LOBSTER. Crete, Greece.[Online]. Available: http://www. ist-lobster. org/publications/presentations/markatosattacks. pdf.

[17] Seitz, L., Pierson, J. M., & Brunie, L. (2003, October). Key management for encrypted data storage in distributed systems. In Second IEEE International Security in Storage Workshop (pp. 20-20). IEEE.

[18] Sen, J. (2015). Security and privacy issues in cloud computing. In Cloud technology: concepts, methodologies, tools, and applications (pp. 1585-1630). IGI global.

[19] Alliance, C. S. (2020). Top Threats to Cloud Computing. [online] Available:https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven; accessed on Mar 16, 2021.

[20] Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

[21] MacAfee, Cloud Adoption and Risk Report. [online] Available: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-cloud-adoption-risk-report-iaas.pdf assessed on 4 Feb 2021.

[22] Singh, S., & Thokchom, S. (2018). Public integrity auditing for shared dynamic cloud data. Procedia Computer Science, 125, 698-708.

[23] Sharma, M. K., & Nene, M. J. (2020). Two-factor authentication using biometric based quantum operations. Security and Privacy, 3(3), e102.

[24] Moutai, F. Z., Hsaini, S., Azzouzi, S., & Charaf, M. E. H. (2019, March). Security Testing Approach for IaaS Infrastructure. In Proceedings of the 2nd International Conference on Networking, Information Systems & Security (pp. 1-5).

[25] Lawal, B. O., Ogude, C., & Abdullah, K. K. A. (2013). Security management of infrastructure as a service in cloud computing.

[26] Cho, Y., Qu, G., & Wu, Y. (2012, May). Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks. In 2012 IEEE symposium on security and privacy workshops (pp. 134-141). IEEE.

[27] Devi, M. G., & Nene, M. J. (2018, March). Scarce Attack Datasets and Experimental Dataset Generation. In 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1112-1116). IEEE.

[28] Yaseen, Q, Jararweh, Y., Panda, B., & Althebyan, Q. (2017). An insider threat aware access control for cloud relational databases. Cluster Computing, 20(3), 2669-2685.

[29] Shishir, K. C. DATA CENTER SECURITY & VIRTUALIZATION. Diss. Touro College, 2018.

[30] Rao, R. G., & Nene, M. J. (2017, March). SEDoS-7: a proactive mitigation approach against EDoS attacks in cloud computing. In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 965-970). IEEE.

[31] Shaikh, A. H., & Meshram, B. B. (2021). Security issues in cloud computing. In Intelligent Computing and Networking (pp. 63-77). Springer, Singapore.

[32] Vaezi, M., & Zhang, Y. (2017). Cloud mobile networks (Vol. 5, No. 3, pp. 23-37). Springer.

[33] Dharmakeerthi, T. D. A Study on Cloud Security Concerns and Resolutions (September 2019).

[34] Ghouse, M., Nene, M. J., & Vembuselvi, C. (2019, December). Data Leakage Prevention for Data in Transit using Artificial Intelligence and Encryption Techniques. In 2019 International Conference on Advances in Computing, Communication and Control (ICAC3) (pp. 1-6). IEEE.

[35] Cullum, p. A survey of the host hypervisor security issues presented in public iaas environments and their solutions.

[36] Halboob, W., Abbas, H., Haouam, K., & Yaseen, A. (2014, August). Dynamically changing service level agreements (SLAs) management in cloud computing. In International Conference on Intelligent Computing (pp. 434-443). Springer, Cham.