ISSN 2278-3091

Volume 10, No.3, May - June 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1441032021.pdf

https://doi.org/10.30534/ijatcse/2021/1451032021

Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward

Hafiz Hasan Naqvi[1], Tahir Alyas[2], Nadia Tabassum[3], Umer Farooq[4], Abdallah Namoun[5], Syed Aun M. Naqvi[6]

[1]Lahore Garrison University, Pakistan,hasannaqvi401@gmail.com

[2]Lahore Garrison University, Pakistan, tahiralyas@lgu.edu.pk

[3]Virtual University of Pakistan, Pakistan, nadiatabassum@vu.edu.pk

[4]Lahore Garrison University, Pakistan, umerfarooq@lgu.edu.pk

[5]Islamic University of Madinah, Madinah, Saudi Arabia a.namoun@iu.edu.sa

[6]Lahore Garrison University, Pakistan, aunnaqvi1994@gmail.com

ABSTRACT

Cloud computing is the emerging platform that is covering individual and corporate needs swiftly. The spread of this global platform is ranging from infrastructure to various middleware, front-end and back-end services. At corporate level, another effective configuration of this phenomenon is multi-cloud environment, which is depicting the ultimate control of the end-user on engaging services from various cloud service providers depending on the service ranking, cost and availability. It is therefore, now very much desirable to have infrastructure services from one service provider while data services are performed on another cloud or having infrastructure services in a distributed environment on multiple clouds. Multi-cloud environment is closely linked with smartly configured security mechanism to ensure the security at rest and in transit. Intrusion detection at various levels and services of cloud platform is not an easy task and when it is spread over multiple clouds then the challenge becomes more complex and tedious. On the other side, managing and integrating a multi-cloud computing environment is also highly complex. From technical point of view, it requires experience and hi-tech skills to formulate sustainable integration between multiple clouds and a coherence among various services to provide an encapsulated platform for the end-user. As in a multicolor environment, the integration can be focused on Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) from various cloud service providers therefore an API-consistent cloud environment is required which leads to the security and more specifically intrusion detection. The problem arises when most of the existing network based intrusion detection systems are designed to deal with the known threats and attacks. These systems are dependent on a rule base that is sufficient to work in certain environment but in case of multi-cloud integration, such fixed rule bases and known-resilience becomes a point of concern. It is therefore, required to look at the intrusion detection system, which may adapt the environmental changes as well as can at least indicate the unknown / anomaly attacks or detection. Honeypot is a vibrant mechanism to divert attention of the unknown attackers and able to capture data to analyze the anomaly. Honeypots may not be so useful independently but along with an intrusion detection system; this mechanism works efficiently and provides tangible results. This research paper is focused on analyzing the multi-cloud environment, intrusion detection systems and the use of honeypots in the existing solutions to understand the possible configurations for effective results in making a sustainable, secure and scalable multi-cloud environment.

.Key words: Security; multi-cloud; honeypots; cloud intrusion detection; ML

1. INTRODUCTION

Cloud computing is the expanding platform with an enormous pace at individual and corporate level or in more precise manner at private and public setups that involves business, corporates as well as governments around the world. The preliminary offering of a cloud platform revolves around three basic service models i.e. Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS), there are certainly hundreds of other services offered by various cloud service providers but all other services are the off shoots of these three basic service models. Global cloud service providers are in a tough competition based on range of services, quality of services, costing and performance [1]. The major cloud service providers include Microsoft

Azure, Google Cloud, Amazon, Oracle, IBM and many more. The basic service models are linked with three operational environments i.e. private cloud, public cloud and hybrid cloud, which are the classification of the accessibility and usage of the said services. Cloud service providers developed their offerings in a systemic manner, but as the user base start expanding, the user start making their own preferences and configurations. Corporates start using multiple or single service from different service providers based on price, quality and performance and start developing their own configuration called multi-cloud environment. This integration has brought many facilities for the end-user as well as many complexities and challenges for service providers as well as end-users [2]. Multi-cloud environment is the distribution of workload between various infrastructures and computation capabilities which provides cost saving, better risk management in terms of disaster mitigation, more flexible business planning and process efficacy. Multi-cloud environment contains complex challenges as well e.g. data accessibility across multiple infrastructures, implementation of consistent data policies for different cloud providers and data availability with a sustainable user base across multi-cloud environment.

Beyond multi-cloud management and configuration, a critical area of concern is the security matters. As the system is spread over various cloud structures using different services and classifications, a certain method of security may not be successful; similarly applying encryption is not suitable that requires ciphering and deciphering everything across multiple system units. In cloud computing the leading security risks include account hijacking, service thefts, insecure interfaces and shared APIs [3]. The consequences of intrusion in multi-cloud environment are having a chain reaction e.g. if intrusion is successful of services than it may lead to the underlying architecture. A penetration at IaaS level means the intruder will have access to virtual machine monitors by working on implementation vulnerabilities that resulted into the modification of virtual machines provided by the IaaS. As cloud itself is a distributed and shared platform therefore, it is not easy to define a security structure for the anomaly detection and privacy management. Another important aspect related to cloud security modeling is the transparency segment focused by the cloud service providers under which they do not allow any customized intrusion detection or security modelling engaging the management service layer that leads to the back channel into the cloud virtual instances. Perhaps that is one of the reasons that most of the intrusion detection systems are tested and implemented over sizeable networks but such deployments and pilot testing on cloud platforms and precisely in multi-cloud environment is yet a highly complex proposition [4].

A honeypot is an intrusion detection and prevention mechanism that is deliberately set up as a decoy to attract and trap the attacker to study in-depth examination of intruders, and discover vulnerabilities in the system to improve the security against latter attacks. It should feel like a real system or server fed up with fake but valuable directories, files, and information that poke the attacker. The server is loaded with monitoring and tracking tools such as firewall and intrusion detection systems, so the traces of activities can be recorded in a log, for detailed analysis. Its key objectives are diverting the attention of hackers from the real network, building their criminal profile, identifying new vulnerabilities and risks, and capturing new viruses or worms for future study. A group honeypot forms a honeynet [5].

Since the conception of digital network and distributed environment, the question regarding the security of data is gaining prominence. In conventional networks, data at rest was the main concern and accordingly various resilience techniques were introduced. Emergence of internet and further introduction of cloud computing from individual to corporate level changed the whole scenario. Data protection, cryptography and security are still important but now a far more important debate is on the prevention of data losses in terms of intrusion detection i.e. to know the anomalies and unknown access to network resources has become a huge domain for researchers and scientists. Various frameworks and methodologies have been introduced. A generic framework for a common intrusion detection framework is mentioned below that depicts the functional modules of intrusion detection. A brief description is given below to deliver the overall concept of CIDF and its functional modulation.

The aforementioned framework consists of E-Box, A-Box, D-Box and R-Box, the purpose and functional properties of these boxes/modules are as follows;

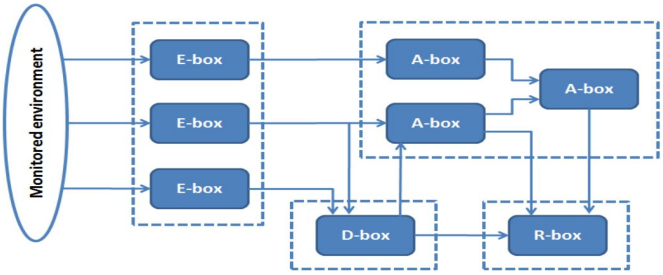

Figure 1: Common Intrusion Detection Framework (CIDF)

Event-box (E-box) contains influx towards a system under observation to collect facts and information for further analysis. Database-box (D-box) keeps that data which is required for processing in A-box and R-box, as shown in the figure 1. d-box receives the data from e-box and provided it to R-box and A-box. The purpose of Analysis-box (A-box) is the processing of instance and evaluation of a potential threat or unknown accessibility pattern to declare it as intrusion for further proceedings. In case of intrusion positive flag, Response-box (R-box) provides the suitable response to the identified threat. CIDF is important because it provides the basic building blocks of any intrusion detection system, therefore, due to its simplicity, CDIF is used as a reference framework to develop more advanced and customizable intrusion detection systems.

As mentioned before that the challenges of multi-cloud environment is the network based intrusion detection in contrast to the host based intrusion detection systems in which the complete focus is on anomaly / threat detection within the host by engaging a rule base and a database of known possible attacks using file system monitoring. It is effective because host traffic is having known signatures while the same application in network intrusion detection system is not successful as the signature of the unknown node/ intruder is not known. The signature dataset will keep showing the positive flag as all the known signatures would be working using the intrusion framework. The solution is to define a usage pattern threshold that helps in alarming on any activity beyond that threshold and take it as a possible threat or intrusion until declared otherwise [6]. The drawback is the problem of false alarm i.e. highlighting valid activities as possible intrusion because the relevant signatures are not the part of dataset, therefore taken as intrusion attempt. In conventional networks it is possible to manage such updates on daily basis but when it is about cloud computing or more precisely multi-cloud environment where authorized and ad-hoc users will be connecting and leaving the network at an enormous pace, such techniques are not suitable [7].

2. LITERATURE REVIEW

Cloud computing with its elasticity, scalability, and availability has changed the overall structure of services and systems. However, the cloud has not fulfilled the expectations of large-scale business organizations. Its major issues are confidentiality, integrity, reliability, and consistency. Inter-cloud as the second layer in cloud computing, by building more dependable cloud services and systems. In it, it is anticipated that client-centric distributed protocols will complement more provider-centric. Inter-cloud storage, which is being implemented, as a ground for dependable services in inter-cloud. It can help in the improvement of confidentiality, integrity, reliability, and consistency [8]. The increase in the popularity of CC is encouraging organizations to shift their data from physical servers to Cloud Servers. However, it comes with a drawback of high costing when switching storage providers. RAID like tactics is implemented on cloud storage. Stripping user's data across various service providers can be handy for customers to avoid provider-lock-in, and it reduces the cost of switching providers. RACS is a substitution that is used to divide the storage load over various providers. Trace-driven simulation is being used to exhibit how RACS has reduced the cost of vendor switching [9]. CC has many advantages, but there is a great issue of security and trust that limits the client. Users often store sensitive data but the providers may be untrusted. A framework is introduced to ensure a secured cloud-database that result into minimizing the security risks. It applied multi-clouds using DepSky, which comprises the combination of clouds in the building of multi-cloud, date, and time constraint validation to eradicate the risk of intrusions, to upraise integrity of data [10]. The practice of CC has increased rapidly in organizations due to its low cost and accessibility. There is a major issue of its security, users store sensitive information but providers may be untrusted. A journey towards multi-clouds has arisen to overcome the issue of security. It is noticed that multi-cloud has reduced the security risk that has shaken the trust of the user [11]. Enterprises are shifting their businesses to online models, provided by Cloud Computing Services Providers (CCSP). None of the CCSP can satisfy all the requirements of its customers. However, they concurrently use services circulated in diverse clouds and set them manually. This convergence causes better results in the integration of multi-clouds. A public cloud integration framework is developed, which is named as CSI-P [12].

Security is the main concern in cloud computing. Multi-cloud has resolved many issues but the security of the data is still in a dispersed and interoperable environment. Following the three steps, can result in the elimination of security risk. Firstly, the private virtual network is introduced to protect the transfer of data. Secondly, an authentication technique is used, based on data encryption, for the protection of the user's identity and his data. Lastly, to discriminate the integrity of data distributed on multi-cloud an algorithm is proposed [13]. The Inter-cloud Federation Framework (ICFF) is an ICAF (Inter-cloud Architecture Framework) component. Problems of multi-cloud computing like interoperability and integration are discussed here. Mainly, there are two types of federations, customer side, and provider side. The inter-cloud architecture system aims to make use of the configuration of cloud resources as the primary working model in an uncoordinated multi-cloud environment. Identity management scenarios and architecture trends provide a framework for federations to implement and provide a stable network for access control [14]. CC has changed application development, deployment, and management. However, IaaS cloud developers come across challenging tasks, to design their applications in cloud providers. Uni4Cloud approach enables to model, configure, and deploy applications to several infrastructure clouds. The main theme is based on CC standards. Such as, Open Virtualization Format and Open Cloud Computing Interface to support interoperability [15]. An open-source strategy is being followed when developing software products. Notwithstanding, integration of different sections in using inappropriate strategy, can be cause different issues. A valuable approach, these issues can be dodged in choosing fitting integration and technique. It examines the constituents of the open-source stage to coordinate choosing a redress integration strategy that can decrease all the exertion. The MELODIC multi-cloud management platform is used to support the stance [16].

Resource management systems handle numerous Cloud Service Providers that need to crack identical interfaces for distinct services, and building covers for the Cloud service APIs. The solution to this is followed by an open-source and retailer platform, which is currently being developed. The middleware includes a multi-agent resource management system for the Cloud. This offers a versatile approach to enveloping existing cloud technologies and emerging tools using a modular architecture [17]. Security challenges are the biggest obstacle in cloud services. CC originates new paths toward security techniques, and architectures such that

partition of application into tiers, and applying cipher on data, we can achieve secure multiple distinct clouds simultaneously [20]. Big Data and Machine Learning are the emerging technologies that can be applied in Multi-cloud systems to produce thrilling results. Locking-in and security problems for providers are major hybrid and multi-cloud concerns. Hybrid systems are tailored to a particular application but are less transportable. They are useful when we have a single task, whereas multi-clouds are fit in where various tasks are required [19].

Multi-cloud is core for sharing resources and security interoperability crosswise various clouds. XACML is broadly used in a distributed environment as a fine-grained but its policy integrations lack formal description and theoretical work. Multi-cloud Access Control Policy Integration Framework consists of the Attribute-based Policy Evaluation Model, Four value Logic with Completeness, and Four value Logic-based Policy Integration Operators. It showed that MACPIF can achieve policy monotonicity, functional extensiveness, canonical fittingness, and canonical completeness [20]. A honeypot is one of the most well known components used to assemble data about assaults and assailants. Notwithstanding, low-communication honeypots just copy a working framework and benefits, and are progressively inclined to a fingerprinting assault, bringing about extreme outcomes, for example, uncovering the character of the honeypot and subsequently finishing the handiness of the honeypot perpetually, or more awful, empowering it to be changed over into a bot used to attack others [21].

The data gathered from honeypots can be used to all the more likely comprehend digital attacks and give bits of information for improving safety efforts, for example, interference disclosure systems. As of late, attacker's innovation has expanded fundamentally consequently, extra and more advanced and explanatory models are required [22]. Security can be achieved through high scalability. Dynamic configuration of honeypot can help IDS and IPS. Eight different methodologies were applied to identify invaders who were utilizing the unsecured network via the unused IP address. These unused IP addresses were directed towards the honeynet server. The result obtained is, intruders find difficulty in gaining information from the network [23]. In network security and network forensics, honeypot and honeynets has become so popular but influenced by various legal and technical issues. One should understand the legal framework of privacy and Legal premises for data processing [24]. A dynamic hybrid honeypot is composed of high and low interaction honeypots. By Scanning and Fingerprinting of an integrated network, a detailed image of the production network and a configuration file for the honeypot are produced. Consequently, more devices can be detected via automated production by the proposed method [25].

If honeypot is not probed, it is worthless and results in dead investment. Previously, a single virtual honeypot deployed in the system that can easily be discovered and compromised. Bringing up multiple virtual honeypots in the network, redirecting every misuse request to a different honeypot could help in reforming the network by improving its vulnerabilities and creating profiles accordingly [26].

3. COMPARITIVE ANALYSIS

Due to the rise of multi-cloud environment various tools and techniques have been introduced to address the respective security issues. Intrusion detection system are evolving as more adaptable and agile black boxes to be configured in accordance with the multi-cloud configuration. Prominent intrusion detection tools like snort (www.snort.org), SPADE (Statistical Package Anomaly Detection Engine), LAD (Login Anomaly Detection), Prelude (www.prelude-ids.org), Stealthwatch (www.cisco.com) revised as CISCO Secure Network Analytics and BreachGate. These and more incoming tools are addressing the security concern of multi-cloud computing by capturing user behavior, login patterns, routine anomalies and on a more detail level they are using distributed architecture with sensors and agents to capture normal and abnormal network behavior. These techniques and tools are further splitting into intrusion detection and intrusion prevention systems with another layer of classification in form of integration tools and service specific tools.

On the other hand, due to the versatility of the multi-cloud security challenges, the intrusion detection debate can be categorized into three main heads i.e. statistical based models and techniques, knowledge based models and techniques and finally machine learning based techniques. For a comparison, let’s have a more closer look into each category. Statistical based models can be further divided into univariate model, multivariate model and time series model. These models are focused on network traffic activity to develop two data sets representing the stochastic behavior. These datasets include different IP addresses, traffic rate, per protocol data packets and rate of connection etc. In case of an instance, one dataset is representing current profile, while the other dataset is the statistical profile of the network. Intrusion is identified by comparing two datasets and the estimation of a score value the threshold level. The knowledge based intrusion detection systems are also further categorized into FSM (Finite State Machine), Description languages (UML) and expert systems. In knowledge based intrusion detection, the network data is captured to identify primary attributes and classes that leads to the development of parameters, classification rules and processes. These models are trained manually by human with the provision of a rule base which provides the standard threshold during the instance of an intrusion detection. The benefit of knowledge based intrusion detection is the reduction in false positives because during training such events are taken care of, yet again beyond training the problem stays there of false alarm. The third category is linked with more advanced techniques using machine learning. It is a continuously expanding category, few of the methodologies are Bayesian networks, Markov Models, Neural Networks, Fuzzy logic, Genetic Algorithms and

Clustering for outlier detection. It requires labelled data, which is resource heavy activity, the purpose of labelled data, is to develop implicit and explicit models to pattern analysis and classification. Machine learning techniques are able to engage models from other categories as well therefore, it is a norm to develop statistical models and implement those models using machine learning techniques to reduce the process costs [19].

For cloud computing in general and specifically for multi-cloud environment there are three prominent contenders that includes HAIL, RACS and ICStore with their respective pros and cons. K.D. Bowers has presented High Availability and Integrity Layer (HAIL) in 2009. HAIL is focused on the file system management across multiple services and servers. It allows user with a set of servers to deal with files without having different protocols and changes. The security methodology of HAIL is using a proxy service on behalf of the user as an identifier. The proxy service / entity communicates with the servers and services spread over multiple cloud platforms by various cloud service providers. HAIL is also efficient in apply encryption in aggregation to ensure the integrity of the files. The strongest part is the aggregation cryptographic protocol which remains active even when the part of file system i.e. a member of multi-cloud is compromised. The limitation of this system is the static management of files without having the functionality to deal with the versioning of files / file system.

Redundant Array of Cloud Storage (RACS) is also managing multi-cloud environment at storage level. The objective of RACS is to keep identifying the most economic and secure resource for the end-user. It works on various parameters like overhead expenses, accessibility and vendor performance. At storage level, RACS is using almost a similar scenario like RAID5 to manage the distributed file management system across various cloud services and service providers. HAIL is also using a RAID like scenario but as mentioned earlier that the tradeoff is between multi-cloud range and versioning. The RAID5 engagement in RACS has established the provisioning of availability, replication and efficiency over multiple cloud systems [27].

The third model is InterCloud Storage (ICStore) presented by Cachin et al. in 2010 for storage services in multi-cloud environment. The objective of ICStore is to maintain confidentiality, integrity, reliability and consistency (CIRC) of data. As compare to previous two models, ICStore is providing more robust security with more precise parameters; the CIRC value is providing the cloud storage services more reliable and practical. ICStore engages the asynchronous fault-tolerant client-driven storage protocols that is moving ahead of RACS and HAIL in terms of the occurrence of a security instance. As mentioned earlier that HAIL provides cryptography for more secure retrieval operations along with erasure-coded distributed storage. HAIL is using symmetric keys that user needs to be kept secret while RACS and ICStore have engaged RAID5 for distribution purpose and to engage multi-cloud environment across multiple servers or multiple services alike.

4. DISCUSSION

The work presented in this paper shows the existing methods and techniques for multi-cloud security regime. It is worth noting that these techniques are showing the limitations and more inclined towards specific scenarios and services. We have provided a comparison of HAIL, ICStore and RACS and all three are storage oriented. In case of single cloud operations, every cloud service provider is having various technologies and to ensure the storage security however, it has also been compromised in various cases. The reason is the very nature of cloud computing i.e. it is highly distributed, ad-hoc and virtualized therefore, conventional methods and security techniques are not providing tangible results. Although as it was discussed that HAIL, RACS and ICStore have provided a solution at multi-cloud level but there is a gap for a comprehensive intrusion detection or more precisely intrusion prevention modulation. It is also important to note that storage related services are not the only services, which are vulnerable in terms of intrusion attacks. As mentioned earlier that APIs, application level operations and hardware resources as well are the targets for intrusion. In a generic form, applications are having trust signature therefore, it is easy for intruders to use applications as a decoy to penetrate into the system as a trusted user, most famous of such intrusion is denial of service attacks, SQL injection attacks and captcha breaking. It is therefore, highly desirable to provide intrusion detection at application level which is more dynamic and challenging.

5. Results

The comparative analysis shows that existing intrusion detection systems are limited in functionality as well as in terms of scope. It is evident that these systems are may be suitable and result oriented for a single cloud deployment but in multi-cloud structure these systems may need to incorporate more robust and dynamic features to deal with not only multiple clouds but also multiple services as shown in Table. 1.

Table 1: Storage Model

Model	Service	Feature	Summary
HAIL	Storage	Encryption Key	Strong security, no versioning
RACS	Storage	RAID5	Strong distribution, low security
ICStore	Storage	CIRC	Strong distribution, reasonable security

6. CONCLUSION

This paper discussed multiple aspects of intrusion and security related to cloud computing. It is important to

consider the expanding segments of intrusion in terms of basic cloud services, data centric attacks and application based penetration. Considering the dynamic nature of multi-cloud environment, it is evident that instead of intrusion detection it is far more important to engage intrusion prevention systems. The statistical, knowledge based and machine learning methodologies are having strong features to be engaged for detection or prevention in terms of predicted attacked patterns and analytics for better management and strategy development for multi-cloud environment. It is recommended to consider such channels that can perform a check-point role for the intruders to observe the anomalies and unknown signatures. The development of such check-points for all type of services and layers SaaS, PaaS and IaaS, honeypots are strong candidates to be considered, linked with machine learning to cluster the upcoming patterns and make the system evolve to enhance the system resilience against intrusion attacks.

REFERENCES

[1] R. Shu and Enck, "A study of security vulnerabilities on docker hub," *In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, no. 5, pp. 269-280, 2017.

[2] Roschke, S., Cheng, F., Meinel, C.: Intrusion detection in the cloud. Dependable, Autonomic and Secure Computing, *IEEE International Symposium*, 729–734 (2009)

[3] Vieira, K., Schulter, A., Westphall, C., Westphall, C.: Intrusion detection for grid and cloud computing. It Professional 12(4), 38–43 (2010)

[4] Lo, C.C., Huang, C.C., Ku, J.: A cooperative intrusion detection system framework for cloud computing networks. In: *Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, ICPPW* '10, pp. 280–284. IEEE Computer Society (2010)

[5] Grance, T., Mell, P.: The nist definition of cloud computing. National Institute of Standards & Technology (NIST) (2011). URL http://www.nist.gov/itl/cloud/ upload/cloud-def-v15.pdf

[6] Garca-Teodoro, P., Daz-Verdejo, J., Maci-Fernndez, G., Vzquez, E.: Anomaly based network intrusion detection: Techniques, systems and challenges. *Computers and Security* 28, 18–28 (2009)

[7] Marinova-Boncheva, V.: A short survey of intrusion detection systems. Problems of Engineering Cybernetics and Robotics (2007). URL http://www.iit.bas.bg/ PECR/58/23-30.pdf

[8] Christian Cachin, Robert Haas, Marko Vukolic, "Dependable Storage in the Intercloud, *IBM Research* – Zurich May 28, 2010

[9] Hussam Abu-Libdeh, Lonnie Princehouse, Hakim Weatherspoon, R,ACS: A Case for Cloud Storage Diversity.*IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 1 (Sep. - Oct. 2013), PP 71-76, Security threat solution over single cloud to multi-cloud using DepSkymodel.

[10] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, Cloud Computing Security: From Single to Multi-Clouds, *45th Hawaii International Conference on System Sciences.*2012

[11] Qing Li, Zeyuan Wang, Weihua Li, Zhichao Cao, Ruiyang Du, Hao Luo, Model-based services convergence, and multi-clouds integration, Computers in industry 64,813-832, 2013

[12] Leila Megouache, AbdelhafdZitouni and MahieddineDjoud, Ensuring user authentication and data integrity in multi cloud environment, Megouache et al. *Human Centric Computing Information Sciences*, 2020

[13] Marc X. Makkes, Canh Ngo, Yuri Demchenko, Rudolf Strijkers, Robert Meijer, Cees de Laat, Defining Intercloud Federation Framework for Multi-provider Cloud Services Integration, 2020

[14] Americo Sampaio, NaborMendonça, Uni4Cloud: An Approach based on Open Standards for Deployment and Management of Multi-cloud Applications, SECLOUD'11, Waikiki, Honolulu, HI, USA Copyright 2011 ACM 978-1-4503-0582-2/11/05, 2011

[15] Kyriakos Kritikos, PawełSkrzypek, Marta Różańska, Towards an Integration Methodology for Multi-Cloud Application Management Platforms, Cloud*ACM Workshop*, UCC '19 Companion, December 2–5, , Auckland, New Zealand, 2019

[16] Victor Ion Munteanu, Calin ¸ Sandru and Dana Petcu, Multi-cloud resource management: cloud service interfacing, Munteanu et al. *Journal of Cloud Computing: Advances, Systems and Applications* 2014

[17] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau, Security and Privacy-Enhancing Multi-cloud Architectures, *Ieee Transactions On Dependable And Secure Computing*, VOL. 10, NO. 4, JULY/AUGUST 2013

[18] Nadia Tabassum, Tahir Alyas, Muhammad Hamid, Muhammad Saleem, Saadia Malik, Zain Ali and Umer Farooq, Semantic Classification Analysis of Urdu English Tweets Empowered by Machine Learning,*Journal of Intelligent Automation & Soft Computing*, Vol. 30, No. 1, 2021

[19] Peng Zhao, Lifa Wu, Zheng Hong, He Sun, Research on Multi cloud Access Control Policy Integration Framework, 3 PANDA Electronics Group Company, limited, Nanjing 210014, China.

[20] Nadia Tabassum, Allah Ditta, Tahir Alyas, Sagheer Abbas, Hani Alquhayz, Natash Ali Mian and Muhammad Adnan Khan, Prediction of Cloud Ranking in a Hyperconverged Cloud Ecosystem Using Machine Learning, *Computers, Materials &*

Continua (CMC), Vol. 67. No. 3. pp. 2585-2600, 2020

[21] DaniyalBaig, Tahir Alyas, Muhammad Hamid, Muhammad Saleem, Saadia Malik, Nadia Tabassum* and Natash Ali Mian, Bit Rate Reduction in Cloud Gaming Using Object Detection Technique, *Materials & Continua (CMC)*, Vol. 67, No.3, 2021.

[22] Leila Megouache, AbdelhafdZitouni and MahieddineDjoud, Ensuring user authentication and data integrity in multi cloud environment, Megouache et al. Human Centric Computing Information Sciences (2020)

[23] Muhammad Adnan Khan, ShaziaSaqib, Tahir Alyas, Anees Ur Rehman, Yousaf Saeed, Asim Zeb, Mahdi Zareei, Ehab Mahmoud Mohamed, "Effective Demand Forecasting Model using Business Intelligence empowered with Machine Learning", *IEEE Access*, 2020

[24] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", *EuroSys'11:Proc. 6thConf. On Computer systems*, 2011, pp. 31-46.

[25] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", *SoCC'10:Proc. 1st ACM symposium on Cloud computing*, 2010, pp. 229-240.

[26] Nadia Tabassum, Allah Ditta, Tahir Alyas, Sagheer Abbas, Hani Alquhayz, NatashAliMianandMuhammad Adnan Khan, Prediction of Cloud Ranking in a Hyperconverged Cloud Ecosystem Using Machine Learning, *Computers, Materials & Continua (CMC)*, Vol. 67. No. 3. pp. 2585-2600, 2020

[27] Javairya Nadeem, Arfan Ali Nagra, Muhammad Asif, Aqsa Iftikhar, Detection of Abnormalities in Real-Time Computer, Network Traffic Empowered by Machine Learning, International Journal of Advanced Trends in Computer Science and Engineering, Volume 10, No.3,