2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-6654-3789-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACITE53722.2022.9823892

The Role of Implementing Cloud Computing Technology for Addressing Critical Security Issues and Overcoming the Challenges Effectively

Melanie Lourens[1]
[1]Department of Human Resources Management
Durban University of Technology, South Africa
Melaniel@dut.ac.za

Manish Kaushik[2]
[2]Professor, Master of Computer Applications, S. S. Jain Subodh P. G. College, Jaipur
mkaushik007@gmail.com

Jayanti Goyal[3*]
[3]Associate Professor, Department of Computer Science, Kanoria PG Mahila Mahavidyalaya, Jaipur, Rajasthan, India

Dr. Rajesh Singh[4]
[4]Professor (Uttaranchal Institute of Technology),
Uttaranchal University, India
drrajeshsingh004@gmail.com

Shikha Kuchhal[5]
[5]Assistant Professor, Department of ECE,
SPITM, DCRUST, Murthal
shikhakuchhal4@gmail.com
0000-0002-2249-4107

Mohit Tiwari[6]
[6]Assistant Professor, Department of Computer Science and Engineering,
Bharati Vidyapeeth's College of Engineering, Delhi
mohit.tiwari@bharatividyapeeth.edu

***Abstract*- The term cloud computing possesses the critical aspect to enhance the network by leveraging the available resources in an effective manner. It has been widely stated that the usage of enhanced IT infrastructure support in realising the goals of the stakeholders in an easier aspect. Cloud computing is a shared pool of operations that is growing in popularity due to its low cost, high efficiency, and high output. Along with its many advantages, cloud computing presents a considerably more difficult scenario in terms of data privacy, intellectual property rights, authenticated access, data security, and so on. Cloud computing technology is becoming ever more challenging in today's society as a result of these challenges. This paper aims to evaluate the security issues in cloud services and implementation of advanced technology to prevent these challenges. In this context, mixed method has been considered (primary quantitative and secondary qualitative) to gather relevant and factual information.**

Keywords: Cloud computing, technology, security, Cloud technology, challenges, Cloud security, security breach.

I. INTRODUCTION

Cloud computing model presents a number of issues for enterprises, particularly safeguarding confidential material such as proprietary information and classified information, as well as personally-identifying relevant data that might fall into the hands of hackers. Possessing critical information freely available online needs a large expenditure in security methods and surveillance of information access. The company may seem to have little knowledge of storing and restoration operations in the cloud computing system, along with limited access to storage solutions. [1]. Cloud computing's novel features, such as multi-tenancy, resource sharing, and remote data storage, have not only put the current security system to the test but have also uncovered new security issues. Safety and confidentiality are the most challenging aspect of cloud computing. A range of security vulnerabilities and issues linked with cloud computing has been investigated recently, the bulk of which affect cloud administration consoles and "virtual machine (VM)" images. The biggest challenges with cloud technology are virtualization and multi-tenancy. Since the cloud is a shared resource platform, organizations must guarantee that all tenant zones are adequately segregated from one another, with no risk of data or activities leaking from one to another. Clients must be able to set up trustworthy virtual domains as well as security zones depending on policies. There may be different data misuse which might impact the delivery of the performance and impact the overall computational element.The problem for software developers in terms of privacy is to build cloud services in such a way that they reduce privacy concerns while yet ensuring legal compliance [2]. There is a risk involved with cloud storage and analysing remotely, as well as growing used of virtualization and platform sharing among users.

The purpose of this paper is to provide a complete review of cloud computing technology and how it may be used to adequately meet security aspects and overcome hurdles.

II. LITERATURE REVIEW

Cloud computing refers to both the program that are made available as resources through the Internet and the equipment and operating system on the systems that provide these functions. The first cloud-like technology ("Cloud 1.0") was created by encapsulating TCP/IP layers, in which networking devices connect with one another using TCP/IP required specifications without knowing where or who the other is. Because of its unique properties, such as dynamically large expansion, adaptability, quantifiable service and self-provisioning of assets, availability as well as internet

connectivity, and a worldwide pool of resource base, cloud computing (CC) has grown increasing popularity [3]. As a consequence, the cloud is an open and shared system, rendering user data security are challenging concern to handle. One of the key benefits of cloud computing is that it can provide a variety of service models based on the needs of customers. Google Apps, Google and Microsoft SharePoint collaboration platform, is an application of a cloud service. IBM, HP, Amazon, Apple, Oracle, and Salesforce are among the companies' providing services. These firms control millions of servers and have made significant investments in cloud computing. Google, which has its own cloud service, is currently the largest provider of cloud computing services.

People presently focus on working in a technological and computer-based world. The Online world has profoundly revolutionised the tech industry, from embedded systems to decentralized computing, utility computing, including revolutionary cloud solutions [4]. Cloud computing is an emerging phenomenon in the world of information technology. Others believe it to be a brand-new discipline of science and engineering. It's a compilation of materials and services that may be accessed over the Internet. As a consequence, "cloud technology" is also known as "Internet computing" in some circles. The word "cloud" refers to a region on the Internet where computation is preloaded and made accessible as a resource.

The hurdles in integrating IoT and Cloud technology have been formally recognised and documented, which will aid academics in finding effective solutions to existing challenges. The correlation of methods provides a path for established opportunities to strengthen their effectiveness. In this part, researchers also highlight potential research topics that, if properly handled, will enable the Cloud-IoT concept to actualize the envisioned safely and securely connected world [5]. The sophisticated identification process for the millions of Connected items that presently exist, as well as the ones that will be added in the future. The context-based solution that provides refers to the ability of IoT items to avoid sending and receiving data between them, their interfaces, and the cloud. There's always been scope for development in terms of network reliability. Cloud computing solutions to function effortlessly. Standardized APIs might be created, allowing third-party apps to be developed. The Internet of Things (IoT) is a network of interconnected devices, each with its own unique address for authentication [6]. When these networked IoT items share communication requests, they are usually needed to verify each other. It's no different with Cloud-IoT, and the same authentication difficulties persist.

Depending on the "Datagram Transport Layer Security (DTLS)" protocol, a "two-way authentication security technique" is designed particularly for IoT. The DTLS protocol is used to connect the network and application layers. This system is developed for the 6LoWPANs and is endorsed by RSA. The researchers' architecture ensures secure communication, secrecy, and legitimacy while keeping end-to-end latency and storage costs to a minimum [7].

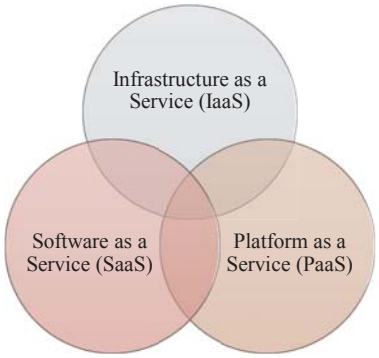

Fig. 1. Three layers of Cloud computing

(Source: Created by Researchers)

Cloud computing could be divided into three tiers based on the different sorts of services available. "***Infrastructure as a Service (IaaS)***", sometimes known as IaaS, is the bottom layer of support and maintenance. PasS – The "***Platform as a Service (PaaS)***" layer is an intermediate layer that provides framework services as well as a host environment for user applications. "***Software as a Service (SaaS)***" is the topmost layer that includes a complete programme that is available as a service on demand. Software infrastructure and platform are all basic computer services [8]. An "X-as-a-Service (XaaS)" paradigm may be used to define service models, where X refers to the computational services. Likewise, service offerings, or Xs, can be represented in any way that is useful to users, including information, security, back-end, and process [9]. Versatile service delivery has dramatically increased the network's service content. Despite the benefits of cloud computing in terms of convenience and flexibility, the adoption of cloud-based solutions is still constrained by security issues. Because of the connected environment, cloud computing implementations are vulnerable to all security breaches [10].

SLAs are used in the cloud computing model to supply services. Performance, reliability, and security objectives should all be covered by "Service Level Agreements (SLAs)". In addition, SLAs specify the penalties that will be enforced if the SLA is broken. Ensuring a strong safety net, as one of the SLA purposes, necessitates a significant increase in resource consumption, which has a negative influence on the performance measure (the more adopted security tools and mechanisms, the worst the impact on the performance of the underlying services) [11]. Using utility functions for security and performance (least security unless otherwise specified), cloud management should examine the trade-off between security and performance [12]. Delivering dynamic security, wherein the much needed controls and protocols can be applied while making other considerations into account, is a more developed idea.

One of the most important security risks as end-users use cloud storage and put their information on the provider's servers is privacy and user data confidentiality. End-users employ cloud-based applications without understanding where the resources for those services are hosted, which could be in other legal regions [13]. When conflicts arise, which are sometimes beyond the control of cloud providers, this offers a promising concern. Information processed at cloud service providers is influenced not only by the standards of the providers but also by the laws of the countries in which the providers are located. Users must agree to the "Terms of

Service" while using such services, which give the services the right to disclose user information in response to legislation and law enforcement inquiries [14].

III. METHODOLOGY

This research paper has considered secondary qualitative method to acquire knowledge regarding security issues in cloud computing technology and strategies to manage. Secondary qualitative on the other hand, has been considered to develop evidence based and theory based information from different journals and articles. Keywords such as security, cloud computing, cloud security are used to search journals and articles from different databases such as Journals, articles.

IV. DISCUSSION AND FINDINGS

As can be seen from the preceding section, researchers have used a variety of strategies and instruments to improve performance and accuracy. Following their research, scientists have provided a set of recommendations. The research should contain a comparison of the success and similarities in the IoT and Cloud computing methodologies. The data were analysed using Tools and Techniques and the Significant Satisfied Aims method. Furthermore, the suggested approach and framework are exact and efficient. Some studies rely on the VM migration approach, AES, ECG technology, MATLAB Fuzzy toolbox, and MATLAB R2017b, as shown in the table. Instead of using a genetic algorithm, iFogSim toolkit uses round-robin strategies to achieve the Significant Satisfied Aims. "Multi-domain IoT Architecture, IoT Management Protocols, and Heterogeneous integrated network resource gathering are examples of additional methods. Resource management algorithm modelling, deep Q-learning based methods, Deep Neural Network, Monte Carlo Tree Search algorithm, XCS learning classifier architecture, and BCM-XCS are also used by certain researchers. Both researchers have strong structures, frames, and functions as a result of their use of this methodology and techniques, including a new method for live VM migration, Workload Aware Virtual Machine Consolidation Method (WAVMCM), a Joint Load Balancing and Mobile Edge Computing (MEC) Offloading Strategy, feedback output based on a Fuzzy algorithm, Fog Computing Allowed Volunteer (VSFC), a novel IoT device for identifying and tracking patients with type-2 diabetes, and novel Software".

Numerous literatures have identified multi-tenancy as a potential threat in cloud computing. Multi-tenancy is a crucial Cloud Computing characteristic that might lead to data vulnerabilities. When it comes to Cloud Computing settings, multi-tenancy is likewise seen as a big danger to both confidentiality and anonymity [15]. Multi-tenancy is a concept used in Cloud Computing to characterise sharing of resources. In Cloud-based (SaaS), where the customer cannot inspect or restrict the source code, multi-Tenancy implies that two or more users are using the same servicing or authorization offered by the "Cloud Service Provider (CSP)" regardless of the specific assets; in this case, multi-Tenancy implies that countless possibly more consumers use the same infrastructure or application.

Authorization helps to define resource access privileges. Authentication in the Cloud-IoT context refers to a three-phase process. The first step would be to develop security policies, which are nothing more than a collection of detailed regulations. The intrusion prevention framework is designed subsequently, followed by the implementation of a system of regulations. The purposes of security models are usually apparent, but the execution of these security standards in the intrusion detection system poses difficulty during the authorization step. However, one of the primary functions of authorized procedures is to simplify regulation enforcement and fill the gap between high-level security regulations and low-level procedures. Authorization standards might be used to assess the policies' completeness and coherence [16]. "Discretionary model DAC", "Mandatory model MAC", "RBAC" and its different variants, "Attribute-based access control model (ABAC)", "BAC model", and "Usage Control (UCON)" are some of the authorization models. In most cases, authorisation models are built around persons, objects, and their interactions. Few authorisation models, meanwhile, are also built on trust, confidentiality, relevance, and expertise. There are many heterogeneity-supportive hybrid architectures in order to suit the organisational demands, specifically in the context of Cloud-IoT [17].

"Man in the Middle attacks (MITM)" is one of the most common types of SaaS assaults. An assailant tries to enter into an ongoing dialogue between a sender and a client in order to insert fake information and get access to the vital data being exchanged. Software alternatives that use powerful encryption technologies, such as "Dsniff, Cain, Ettercap, Wsniff, Airjack, and others", have been designed to safeguard against them [18]. Shared and non-shared networks, public and private networks, small space and large space networks, and so on are all considered as having different security challenges to cope with [19]. While ensuring security measures, Researchers consider the following points: network secrecy and integrity, adequate access control, and maintaining security against independent third hazards [19]. "DNS assaults", "Sniffer attacks", "reused IP address issues", "Denial of Service (DoS)" and "Distributed Denial of Service (DDoS)" attacks are all examples of network security issues.

Virtualization has evolved into a critical component of cloud computing during the last few years. As virtual machine technology grows increasingly ubiquitous in the IT world, VM security has become a major problem. Virtualization creates a more difficult and dangerous security posture. Studies investigated security flaws in virtualized environments and draw conclusions on a few security issues. "Denial of service (DOS)" vulnerabilities are one example. "Virtual machines (VMs)" and the host share resources such as CPU, memory, disc, and network in a cloud platform. As a result, it's feasible that VMs will be subjected to a DOS, which will use all of the host's resources. As a result, the system will decline any requests from outsiders due to a lack of resources [20].

Since Cloud-IoT links actual items to the network interface, privacy and confidentiality concerns are significant, and this inclusion may be harmful at times even though it is so closely tied to the user and smart devices that monitor user actions. More effort may be placed into developing mechanisms for more successfully enforcing safety requirements and preventing unauthorised access [20]. On the other hand, adversaries keep on trying to attack systems, such as implanting spyware into devices or interfering with data stored in the cloud. In the Cloud-IoT scenario, access points are extremely important for safeguarding and mitigating side-channel risks.

Although the mentioned security vulnerabilities have remedies, many of which are only targeted at some areas of

the issues, this does not mean that the cloud computing system as a whole is protected. Some security standards must be met by a secure cloud computing platform. The "International Standards Organisation (ISO)" has proposed various information security principles, which should also be used to govern cloud security. Confidentiality and integrity are two of these measures designed to prevent data breaches [21]. Based on its proposed scheme, Non-Repudiation, Availability, and Identification & Authentication these security requirements address several security aspects of cloud computing.

V. CONCLUSION

Thus, it has been concluded that huge growth in the implementation of IoT in recent years, and it is constantly extending its participation in all imaginable parts of the physical world. IoT will create a large quantity of data in the next years, which will need to be gathered and processed correctly for delivering enhanced services. The combination of IoT and Cloud is emerging to be a viable approach for handling the vast amounts of data generated by millions of various systems which are connected . The implementation of Cloud-IoT, on the other hand, is hampered by a number of obstacles from many angles. In this study, researchers highlight key Cloud-IoT problems before concentrating on security concerns and approaches. Moreover, this paper has identified about the open concerns and constraints in the Cloud-IoT space. Finally, they discussed potential research paths that may help to develop Cloud-IoT technologies. The commercial industry is increasingly using cloud computing technologies to boost the effectiveness of financial operations, corporate governance, and business procedures. This is happening at a faster rate in industrialised countries like the United States, Canada, and the United Kingdom. The commercial sector's use of cloud technology necessitates careful consideration of factors such as the most appropriate secure cloud deployment type, service-level agreements, and cloud operator. There are many different types of cloud solutions, hence determining migration capability and choosing a suitable provider is crucial, since this will affect the interests of stakeholders such as financial institutions. Cloud computing is the use of shared computer virtual resources on a demand basis. When these services are used correctly, they can cut costs and management duties while also boosting an organisation's efficiency, agility, and performance. Cloud computing, on the other hand, faces a number of obstacles, including data security and privacy concerns.

VI. ACKNOWLEDGEMENT

I would like to thank my professor for hiding me throughout the research work and helping me to complete this work effectively. I am also grateful to my family and friends who remain a constant source of support to me.

REFERENCES

[1] Rong, C., Nguyen, S.T. and Jaatun, M.G., 2013. Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), pp.47-54.

[2] Sun, X., 2018, May. Critical security issues in cloud computing: a survey. In 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 216-221). IEEE.

[3] Tadapaneni, N.R., 2018. Cloud Computing: Opportunities And Challenges. Available at SSRN 3563342.

[4] Zhang, N., Liu, D. and Zhang, Y., 2013, November. A research on cloud computing security. In 2013 International Conference on Information Technology and Applications (pp. 370-373). IEEE.

[5] Haimes, Y.Y., Horowitz, B.M., Guo, Z., Andrijcic, E. and Bogdanor, J., 2015. Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems. Systems engineering, 18(3), pp.284-299.

[6] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.

[7] Ramgovind, S., Eloff, M.M. and Smith, E., 2010, August. The management of security in cloud computing. In 2010 Information Security for South Africa (pp. 1-7). IEEE.

[8] Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B., 2013. An analysis of security issues for cloud computing. Journal of internet services and applications, 4(1), pp.1-13.

[9] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.

[10] Wu, H., Ding, Y., Winer, C. and Yao, L., 2010, November. Network security for virtual machine in cloud computing. In 5th International conference on computer sciences and convergence information technology (pp. 18-21). IEEE.

[11] Nguyen, K.K., Hoang, D.T., Niyato, D., Wang, P., Nguyen, D. and Dutkiewicz, E., 2018, April. Cyberattack detection in mobile cloud computing: A deep learning approach. In 2018 IEEE wireless communications and networking conference (WCNC) (pp. 1-6). IEEE.

[12] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Fiber Matrix Composite through Electric Discharge Machining: A short review" Material Today Proceedings, https://doi.org/10.1016/j.matpr.2021.07.288

[13] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Metal Matrix Composite Using Electric Discharge Machining: A Short Review" Evergreen, 8 (4), pp.740-749.

[14] Sadeeq, M.M., Abdulkareem, N.M., Zeebaree, S.R., Ahmed, D.M., Sami, A.S. and Zebari, R.R., 2021. IoT and Cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, 1(2), pp.1-7.

[15] Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F. and Egelman, S., 2019. Privacy and security threat models and mitigation strategies of older adults. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 21-40).

[16] V. Panwar, D.K. Sharma, K.V.P.Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations And Optimization Of Surface Roughness In Turning Of EN 36 Alloy Steel Using Response Surface Methodology And Genetic Algorithm" Materials Today: Proceedings, Https://Doi.Org/10.1016/J.Matpr.2021.03.642

[17] A. Jain, A. K. Pandey, (2019), "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191. https://doi.org/10.1016/j.matpr.2019.06.292

[18] A. Jain, A.K.Yadav & Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684. https://doi.org/10.1016/j.matpr.2019.12.010

[19] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084- 8045.

[20] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations In Electrical Discharge Drilling Of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261. https://doi.org/10.1016/j.matpr.2017.07.054

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