2023 Sixth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU) | 978-1-6654-7723-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/WiDS-PSU57071.2023.00034

Trust Management Frameworks In Multi-Cloud Environment: A Review

Arwa Alajroush
College of Computer and Information Sciences
Prince Sultan University
Riyadh, Saudi Arabia
221421241@psu.edu.sa

Dr. Rabia Latif
Artificial Intelligence and Data Analytics Lab
College of Computer and Information Sciences
Prince Sultan University
Riyadh, Saudi Arabia
rlatif@psu.edu.sa

Dr. Tanzila Saba
Artificial Intelligence and Data Analytics Lab
College of Computer and Information Sciences
Prince Sultan University
Riyadh, Saudi Arabia
tsaba@psu.edu.sa

***Abstract*— The term "cloud computing" refers to a method of managing and using resources remotely. Networks, servers, applications, machines, and other resources and storage are all part of the shared and virtualized resource pool that is offered. In addition to providing the flexibility, stability, and scalability many organizations need the services of cloud computing, this reduces the need for setting up the private cloud and deploy separate hardware resources. However, multi-could settings presented several security and trust issues. This paper primary contribution is an examination of contemporary, serious trust challenges that arise in a multi-cloud context. And to put out a survey comparing trust management frameworks for Multi-Cloud environment to address the challenges identified. The suggested solution is given to have a more robust and secure trust framework based on data compliance.**

Keywords—Cloud Computing, Trust Issues, Multi-cloud

I. Introduction

Cloud Computing has become one of the essential services due to features like providing resources with limited management and involvement of cloud service providers (CSPs). Cloud Computing can be defined as an approach of handling and accessing recourses remotely by providing a pool of shared and virtualized resources which includes networks, servers, application, machines, storage and other resources. [1]

Cloud offers three types of services: [2] Software as a Service (SaaS): is an approach entails distributing Internet-based on software to various businesses that will be paid for either a subscription basis or on a per-use basis. SaaS is suits short-term initiatives since it is managed from a single location, allowing businesses to focus on other matters. Secondly, Infrastructure as a Service (IaaS): which provides the fundamental infrastructure of virtual servers, networks, operating systems, and storage devices. This eliminates the necessity for office hardware while delivering the flexibility, dependability, and scalability many businesses want from the cloud [3] Lastly, Platform as a Service (PaaS): where the infrastructure and software are deployed by cloud providers, but businesses may create and use their own apps. With PaaS, web applications may be produced rapidly and easily because of the service's flexibility and dependability. If several developers are working on a single project, PaaS solutions are scalable and appropriate. Additionally, it is helpful when utilizing a trusted data source. IaaS is the most popular Cloud Computing service model.

In recent years not only the usage for cloud has increased but the usage of Multi-Cloud environment, which generally refers to the consumption of cloud services from two or more public cloud providers. Most organizations embrace Multi-Cloud models as part of their resources because of the benefit they gain from it such as increasing robustness and dependability, cost savings, and risk reduction [4].

Yet, several security and trust challenges arise with multi-could environments such as how to select a trust worthy CSPs, how to control the flow of trust information, the lack of consistency and the overlaps between CSPs policies, how to assess and define trust in light of the particular characteristics of the Cloud Computing setting, how to ensure the security of data while storing and exchanging it , and how to take into account and offer various degrees of service security in accordance with the degree of trust.

The main contribution of this paper is to compare current trust frameworks in multi-Cloud environment, to identify their strength weaknesses and the current gaps.

II. Background

A. Cloud computing

The definition of cloud computing has been address by a large number of researchers Stanoevska-Slabeva and Wozniak [5] studied the different definition and came with the conclusion that cloud computing have the following features: A whole new model for computers is cloud computing. X-as-a-Service refers to the provision of applications and structure resources (hardware, storage, and system software). Pay-per-use business models are the foundation of cloud computing whether these services are delivered by a third party provider or to external customers. Clouds' major attributes are virtualization and dynamic scalability on demand. Even though utility computing can be utilized on its own, SaaS and utility computing are supplied together. The use of cloud services can be done via an API or a web browser. based on that we define cloud computing as a technique for managing and gaining access to resources remotely by offering a pool of shared and virtualized resources that includes networks, servers, applications, computers, and other resources and storage. which be accessed through API or web. Cloud computing services can be offered as a Software as a Service (SaaS), Infrastructure As A Service (IaaS) and Platform As Services (PaaS).

978-1-6654-7723-9/23/$31.00 ©2023 IEEE
DOI 10.1109/WiDS-PSU57071.2023.00034

B. *Multi- Cloud Environment*

According to Gurusamy and Elemo [6] In the multi-cloud model, various SaaS, PaaS, and IaaS services are made accessible to the business on demand from a number of cloud service providers. Nowadays, companies are not dependent on a single cloud service provider. In addition to using public clouds, businesses may also use private ones. It is clear that in a multi-cloud environment, the user or company uses several cloud services for various business applications. For instance, they may use a private cloud to store data and still another cloud to analyze and share the data [7].

C. *Trust Issues*

Trust is viewed as a quantitative notion that uses experience to enable people to form trustworthy opinions. A robust foundation is provided by authorization and other traditional strict security measures, but they fall short when participating organizations engage in harmful activity. Trust as a soft social security concept may be able to address these security issues by forbidding malicious entities from engaging in interactions, which creates a highly trustworthy cloud computing environment [Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments].

Because cloud services are an Internet-based application, corporations have access to a lot of private information, and data transportation across the Internet mostly rely on "trust" between service user and provider. However, security issues frequently emerge when privacy is violated [8].

III. Related Work

Having a trusted cloud services has grown to be a significant problem in cloud environments in recent years. Researcher used several approaches to solve and enhance it.

Witt et al [11] enhanced business model adds security features like where they introduced a security governance framework for a Multi-Cloud, the framework addresses the necessity to incorporate security and business needs in one framework for Multi-Cloud environment. the framework applies the security needs using Business Process Model and Notation (BPMN) to reach a security business governance, the paper addressed different security issues in multi-Cloud environments such as the conflict between CSPs in policies and SLAs and the absence of interoperability, the authors also discussed some of the related security requirements like Availability, Integrity, Accountability and Privacy. additionally, a straightforward illustration case was proposed for business process model used for customer relationship management (CRM) provisioning services from client requests using BPMN notation to demonstrate the objective of their approach.

Rios et al [12] and Latif et al [13] presented an SLA based frameworks, where Rios et al [12] Proposed a brand-new technique for MUSA SLA-based security and privacy assurance framework in Multi-Cloud combines security by design, privacy by design as well as operational quantified assurance. The proposed framework was evaluated in two different scenarios: Flight scheduling application and Tampere Smart Mobility (TSM).

Latif et al [13] presented an original trust framework for federated cloud environment based on Service Level Agreement (SLA) and CSPs' feedback. The SLA method was tested where they had 8 selected factors to evaluated and enhance trust, each factor has a weight and the final SLA score get calculated based on that. The second method is based on the user's feedback where a survey was conducted with 6 users, the survey consisted of thirty questions about the selected CSP. After that a comparison with the existing methods was conducted where their framework outperformed other methods.

LI et al [14] offered a novel framework based on trust and reputation assessment to evaluate the trustiness, where the framework examines the level of security using a security metrics specific to clouds. The reputation-based trust evaluation approach uses feedback ratings on cloud service quality to evaluate a cloud service's reputation. The researchers used a real-world web service dataset to test the framework where it outperformed the other compared methods.

Lastly, Mehraj and Banday [15] studied trust issues in cloud, then they introduced a zero-trust framework based on authorization for cloud taking in consideration both the CSPs and clients. the framework consists of the following stages: sensitive data identification, maps flows of the identified data, user authorization, device authorization, access control, zero-trust boundary, security of application, monitoring and finally automation of security tools. the authors are aiming to test the framework in future work.

TABLE I. SUMMERY OF LITERATURE REVIEW

Reference	***Used Method***	***Summery***	***Weakness***
[11]	Enhanced Business Process Mode and Notation (BPMN)	provided a security governance framework for a multi-cloud environment, addressing the requirement to combine security and business demands in a single framework.	Given the multi-cloud environment, the security needs were not integrated in the proposed framework.
[12]	MUSA SLA-based	Proposed a technique for MUSA SLA-based security and privacy assurance framework in Multi-Cloud combines security by design, privacy by design as well as operational quantified assurance.	This framework's rules and constraints will affect both new and existing applications and may necessitate substantial changes to current

Reference	*Used Method*	*Summery*	*Weakness*
			systems and data flows.
[13]	(SLA) and CSPs' feedback Based	Proposed a trust framework for federated cloud environment based on Service Level Agreement (SLA) and CSPs' feedback.	The zero trust concept was not included in the framework, hence it cannot be guaranteed.
[14]	Reputation and feedback based	Proposed a novel framework based on trust and reputation assessment to evaluate the trustiness, where the framework examine the level of security using a security metrics specific to clouds.	The proposed framework was not implemented in Cloud environment.
[15]	Zero-trust Based	introduced a zero-trust framework based on authorization for cloud taking in consideration both the CSPs and clients.	The framework was not tested

IV. Discussion

The reviewed literature leads to the conclusion that the current models have certain advantages as well as disadvantages. There are limitations in using compliance to address and resolve trust issues in Cloud and Multi-Cloud environments where there is only limited amount of research in that area, the mentioned research lacks verification and testing as showing in Table 1. Consequently, a new compliance-based framework must be proposed to fill the current gap.

V. Propsed Framework

Because multi-Cloud systems are dynamic heterogeneous settings, adhering to security measures might lessen current trust problems like policy conflicts, data ownership and secure data exchange. Numerous features and approaches have been proposed by researchers to overcome these problems, but no one solution can satisfy all of the criteria.

As a result, the solutions that researchers have proposed frequently do not cover all of the requirements to increase the trust and maintain data security. Furthermore, given the dearth of research linking compliance with resolving trust concerns, this paper aims to close that gap by adopting that strategy and establishing a compliance-based framework in the future.

Figure 1 shows a flow chart of the suggested framework where users can choose a trustworthy CSP by comparing a trust value with a trust threshold, the trust value is calculated based on two trust factor the first one is SLA Value , the Second one is based on compliance value, the compliance value measures the CSP compliance controls that we will propose based on threat in Multi-Cloud environments.

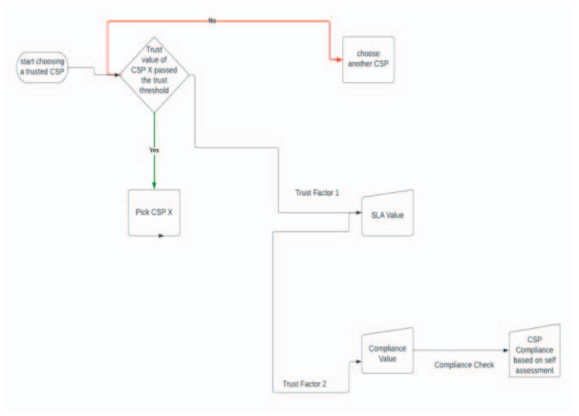
start choosing a trusted CSP
No
Trust value of CSP X passed the trust threshold
choose another CSP
Yes
Pick CSP X
Trust Factor 1
SLA Value
Trust Factor 2
Compliance Value
Compliance Check
CSP Compliance based on self assessment

Figure 1: Suggested Compliance-based Framework

Each CSP should publish a self-assessment with the compliance controls and based on that, compliance value will be calculated, Users can then select a trusted CSP.

In the future, we will work on enhancing this framework and evaluate it using cloud simulator or case studies. Comparison will be done to show the efficiency of the proposed framework.

VI. Conclutison

The term "cloud computing" describes the utilization and management of distant resources, including networks, servers, PCs, applications, and other resources and storage. Businesses are very interested in the flexibility, reliability, and scalability that cloud computing services provide. Investigating the major trust challenges that are now present in a multi-cloud scenario is the main contribution of this article. To address the issues raised, a research comparing trust management solutions ought to be released.

References

[1] C. W. a. E. C. Tharam Dillon, "Cloud Computing: Issues and Challenges," in 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[2] P. Sareen, "Cloud Computing: Types, Architecture, Applications,," International Journal of Advanced Research in, vol. 3, no. 3, 2013.

[3] D. R. D. B. B.Kezia Rani, "Cloud Computing and Inter-Clouds - Types, Topologies and Research Issues.," in Procedia Computer Science 50, 2015.

[4] Jiangshui Hong, "An Overview of Multi-Cloud Computing," in Workshops of the international conference on advanced information networking and applications , 2019

[5] Stanoevska-Slabeva, K., & Wozniak, T. (2010). Cloud basics–an introduction to cloud computing. Grid and cloud computing, 47-61.

[6] "Direct-Cloud, Multi-Cloud, and ConnectedCloud – Terminologies Make a Move in".

[7] Hong, J., Dreibholz, T., Schenkel, J. A., & Hu, J. A. (2019, March). An overview of multi-cloud computing. In Workshops of the international conference on advanced information networking and applications (pp. 1055-1068). Springer, Cham.

[8] Rahi, S. B., Bisui, S., & Misra, S. C. (2017). Identifying the moderating effect of trust on the adoption of cloud ‐ based services. International Journal of Communication Systems, 30(11), e3253.

[9] C. G. G. a. E. B. Hamad Witti1, "A Conceptual Framework of Security Requirements in Multi-cloud Environment," World Congress on Services, no. Springer, pp. 3-17, 2018.

[10] E. I. X. L. M. R. W. M. J. D. Erkuden Rios, "Service level agreement-based GDPR compliance and security assurance in (multi)Cloud-based systems," IET Software, vol. 13, no. 3, pp. 213-222, 2019.

[11] S. H. A. S. L. Rabia Latif, "A novel cloud management framework for trust establishment and evaluation in a federated cloud," The Journal of Supercomputing, vol. 77, no. 11, p. 12537–12560, 2021.

[12] Q. W. ,. X. L. X. C. N. Z. XIANG LI, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of," IEEE Access , vol. 7, pp. 9368 - 9383, 2019.

[13] M. T. B. Saima Mehraj, "Establishing a Zero Trust Strategy in Cloud Computing Environment," in 2020 International Conference on Computer Communication and Informatics, 2020.