**Distributed trust protocol for IaaS cloud computing**

**Literature Review**

**Group Members:** Nimra Amer (21L-5609)

Muhammad Ahmad (21L-5617)

**Section:** BS(DS)6A

**Submitted To :**  Professor Danyal Farhat

**Introduction**

IaaS in cloud computing offers infrastructure for accessing networks, servers, virtual machines, and data. Distributed trust protocols ensure security and privacy by establishing trust between consumers and providers through encryption, authentication, and access controls.

**Gaps in the Research Papers**

**Bridging the Gap: Shared Responsibility for IaaS Security**

The collaboration between cloud providers and consumers is crucial, yet often leads to trust protocol violations. Pascal M. Mutulu emphasizes the top priority for cloud providers should be ensuring the security of consumer/user data in IaaS. However, there's a research gap in understanding the persistent misbalance in the latest IaaS cloud infrastructure. This gap stems from the misconception that security is solely the responsibility of cloud providers, neglecting users/consumers. Security issues must be tackled collaboratively by both parties to prevent data leaks and maintain the security of personal virtual machines.

**Insufficient practical Implementation details**

The authors [2] introduce the Distributed Trust Protocol for IaaS computing to mitigate trust issues. However, it lacks detailed information on its practical implementation. This review aims to fill this gap by exploring the practical aspects of implementing the protocol, including potential challenges, technical specifications, and how it addresses trust issues in the IaaS cloud computing environment.

**Comparative Analysis with Centralized Protocols:**

The author [3] highlights that conventional trust evaluation protocols are typically centralized and one-way. A potential gap lies in the absence of a comprehensive comparative analysis that explores the advantages and disadvantages of centralized versus distributed trust evaluation protocols within the context of Intercloud. The need for Intercloud utilization is not addressed, and there is no mention of the types of Intercloud.

**Implementation and Integration Challenges**

The authors [4] discuss the concept of distributed trust protocol, but it does not provide implementation details or guidelines on how to integrate it with IaaS computing. This creates a potential gap. Additionally, the text does not specify whether the protocol aligns with established standards or frameworks, which could hinder its adoption and integration within the broader ecosystem of IaaS cloud computing.

**Specific Security Concerns**

The authors mention [2] security concerns in adopting cloud computing and also discuss the concerns that cause trust issues in adopting cloud computing. The gap here is that the nature of these concerns is not specified. A more detailed exploration of the specific security challenges faced by enterprises when adopting cloud services could enhance the understanding of the problem.

**User Experience in Customized Trust Evaluation**

The literature [3] introduces an innovative mechanism for storing feedback to facilitate customized trust evaluation. "Third, to facilitate customized trust evaluation, an innovative mechanism is used to store feedback, such that it can be processed flexibly while protecting feedback privacy." However, there is a potential gap in the discussion regarding the user experience implications and usability of this mechanism. The emphasis should be on understanding how users interact with the system, the intuitiveness of the feedback processing, and any challenges related to user adoption.

**References:**

[1] Pascal M.Mutuli , “A Multi Tendance Cloud Trust Model using Quality of Service Monitoring: A case of Infrastructure as a Sevice” , Distributed Computing Technology of the University of Nairobi , 2020 , P53/10982/2018

[2]U. A. Kashif, Z. A. Memon, A. R. Balouch and J. A. Chandio, "Distributed trust protocol for IaaS Cloud Computing," 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2015, pp. 275 279,doi:10.1109/IBCAST.2015.7058516

[3] Y. Dou, H. C. B. Chan and M. H. Au, "A Distributed Trust Evaluation Protocol with Privacy Protection for Intercloud," in Transactions on Parallel and Distributed Systems, vol. 30, no. 6, pp. 1208-1221, 1 June 2019, doi: 10.1109/TPDS.2018.2883080.

### [4] Meenu Dave, Archana B. Saxena “IaaS service in the public domain: impact of various security components on trust”, AISC vol 933 doi: 10.1007/978-981-13-7166-0\_79