**---------------------------------------------------------------------------------------------------------------------**

**Parallel and Distributed Computing**

**---------------------------------------------------------------------------------------------------------------------**

**Project Phase: 2**

**---------------------------------------------------------------------------------------------------------------------**

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

Muhammad Ahmad (21L-5617)

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

**Submitted To:**  Professor Danyal Farhat

**Distributed trust protocol for IaaS cloud computing**

**Introduction**

Infrastructure as a Service (IaaS) is a vital component of cloud computing. Amazon introduced it in 2006, and it has revolutionized the way people and businesses access and utilize computing resources. IaaS allows users to access virtualized servers, storage, and networks whenever required, enabling them to create and manage their virtual machines based on their needs. This model offers exceptional flexibility and scalability, allowing users to customize their computing infrastructure to meet their specific requirements without the burden of owning physical hardware. Essentially, IaaS democratizes computing power, making robust IT resources available to anyone with an internet connection.

However, the centralized and distributed nature of IaaS computing can result in various threats or malfunctions, leading to trust and security issues. These issues, such as data leakage, unauthorized access, hacking, or other threats, can arise due to shared physical storage among many users in IaaS environments. This higher probability of threats occurring disrupts the distributed trust protocols of IaaS computing.

In this paper, we bridge the gap by offering detailed insights into the practical implementation of the Distributed Trust Protocol for IaaS computing. We conduct a comparative analysis of centralized and distributed trust evaluation protocols within the Intercloud context, explore implementation challenges, discuss specific security concerns, and examine the user experience implications of customized trust evaluation mechanisms.

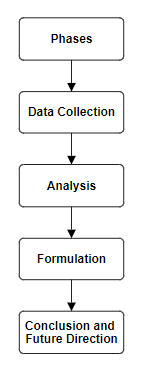
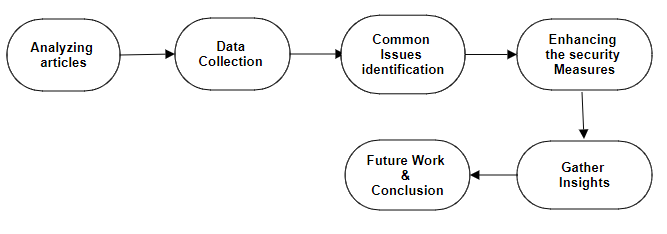
This paper is further organized as follows: the literature review is presented in Section 2, research methodology and scope of work presented in Section 3, implementation details in Section 4, results obtained in Section 5 followed by conclusion and future direction in Section 6.

**3. Research Methodology**

In this section, we present the flowchart of the methodology used in the research work. Along with that we also discuss the scope of the work presented.

* **Research Methodology Flowchart:**

In the first phase, we reviewed different research articles to understand the implementation details of distributed protocols for IaaS computing and identify trust protocol deficiencies. In the second phase of our research methodology, we embarked on a data gathering process meticulously designed to capture relevant insights from trustworthy sources. We sought out data that would provide a deep understanding of user interactions within IaaS environments, aiming to uncover any security vulnerabilities present. By examining user experiences, we aimed to shed light on their interactions with the platform, identifying potential points of weakness such as instances of unauthorized access, breaches of personal space, and incidents of data leakage. This data collection phase served as a crucial foundation for our subsequent analysis and strategic planning efforts, enabling us to formulate targeted solutions to enhance security within IaaS environments. Finally, we formulated a strategic plan to enhance security measures within IaaS environments, addressing identified deficiencies and strengthening trust protocols.



* **Scope of the Work:**

This research analyzes implementation details, user experiences, and security challenges of distributed trust protocols in IaaS cloud computing. It proposes practical measures to enhance security and addresses identified deficiencies. The findings will improve the overall security of IaaS environments. Key references include seminal works on cloud computing security [1] [2], and recent studies on distributed trust protocols [3].

**References:**

[1] Ristenpart, T., et al. (2009). Exploring information leakage in third-party compute clouds. In Proceedings of CCS '09.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. NIST Special Publication 800-145.

[3] Rahman, M. A., & Rahman, M. A. (2020). A Survey on Security and Privacy Issues in Cloud Computing. arXiv:2010.03875.