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

**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.

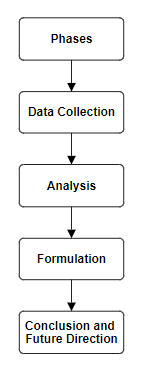
In this paper, we bridge the gap by offering detailed insights into the practical implementation of the Distributed Trust Protocol for IaaS computing. We conduct a comparative analysis of centralized and distributed trust evaluation protocols within the Intercloud context, explore implementation challenges, 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.

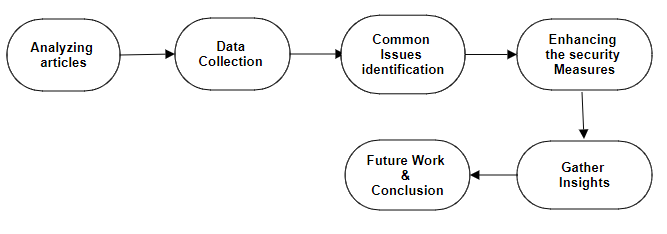
**3. Research Methodology**

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:**



1. In the **Initial Phase** of our research methodology, we conducted an extensive review of various research articles to comprehensively understand the intricate implementation details of distributed protocols tailored for Infrastructure as a Service (IaaS) computing. This phase not only allowed us to gain profound insights into the underlying mechanisms of these protocols but also facilitated the identification of potential deficiencies in existing trust protocols within the IaaS ecosystem. By scrutinizing the literature, we aimed to pinpoint areas where trust might be compromised, thus laying the groundwork for our subsequent investigations.
2. Transitioning into the **Second Phase**, we meticulously embarked on a data-gathering endeavor, carefully curated to capture insights from reputable and trustworthy sources. Our approach was meticulously designed to capture a multifaceted understanding of user interactions within IaaS environments. We delved into a variety of data sources to uncover nuances in user experiences, aiming to unearth potential security vulnerabilities lurking within these environments. Through this meticulous examination, we endeavored to shed light on user 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 comprehensive data collection phase served as a crucial foundation for our subsequent analytical endeavors. Armed with rich insights gleaned from user experiences, we embarked on a rigorous analysis aimed at distilling meaningful patterns and trends. By scrutinizing the collected data, we sought to unravel underlying factors contributing to security vulnerabilities within IaaS environments. This analytical phase facilitated a nuanced understanding of the challenges at hand, paving the way for the formulation of targeted solutions to enhance security measures.
3. Finally, in the **Last Phase** leveraging the insights garnered from our analysis, we devised a strategic plan aimed at bolstering security measures within IaaS environments. Our plan was meticulously crafted to address identified deficiencies and fortify trust protocols, thus fostering a more resilient and secure computing environment. By delineating actionable steps and strategic interventions, we aimed to instill confidence in stakeholders and mitigate potential risks effectively. This strategic planning phase represents a culmination of our research efforts, encapsulating our commitment to advancing security within the realm of IaaS computing.



* **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.