Distributed Trust Protocol for IaaS Cloud Computing

Muhammad Ahmad
FAST School of Computing
FAST NUCES Lahore
Lahore, Pakistan
l215617@lhr.nu.edu.pk

Nimra Amer
FAST School of Computing
FAST NUCES Lahore
Lahore, Pakistan
l215609@lhr.nu.edu.pk

Danyal Farhat
Faculty of FAST School of Computing
FAST NUCES Lahore
Lahore, Pakistan
danyal.farhat@lhr.nu.edu.pk

***Abstract*--Infrastructure as a Service is a cloud computing service that provides users as-a-service access to virtualized computing resources instead of requiring physical ownership of the hardware. Due to the distributed nature of IaaS, security and trust challenges such as data leakage and unauthorized access to data require robust trust evaluation. The Distributed Trust Protocol offers a viable solution to these challenges. The current paper presents the proposal and realization of the Distributed Trust Protocol for IaaS settings. First, it clearly outlines a comparison of centralized and distributed trust evaluation approaches in the context of Intercloud to demonstrate the advantages of decentralized trust management. Second, the paper provides an extensive practical implementation of the protocol that considers critical implementation issues and uses advanced cryptographic methods and decentralized architectures. This research would advance the knowledge in the field of trust protocol in cloud computing and its implementation, especially in distributed and decentralized settings such as IaaS. Highlighting the need for trust evaluation and presenting real-world solutions, the study endeavors to enhance security policy and encourage the use of secure cloud computing.**

Keywords—Infrastructure as a Service (IaaS), cloud computing, trust evaluation, Distributed Trust Protocol (DTP), Intercloud, security, implementation challenges

1. Introduction

Infrastructure as a Service (IaaS) is a vital component of cloud computing. Amazon introduced it in 2006, revolutionizing how 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 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 are presented in Section 3, implementation details in Section 4, results obtained in Section 5, conclusion and future directions in Section 6, followed by references in Section 7.

2. Related Work

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 that cloud providers' top priority should be ensuring consumer/user data security 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 integrating 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.

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:**

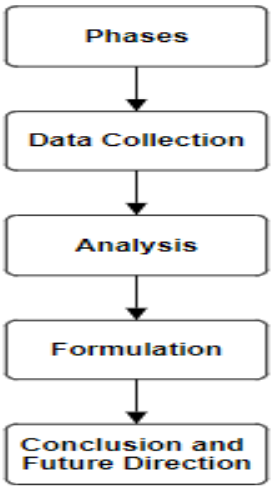

Fig1 Flowchart

1. **First Phase**

In this 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. **Second Phase**

Transitioning into the next 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. **Third Phase:**

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.

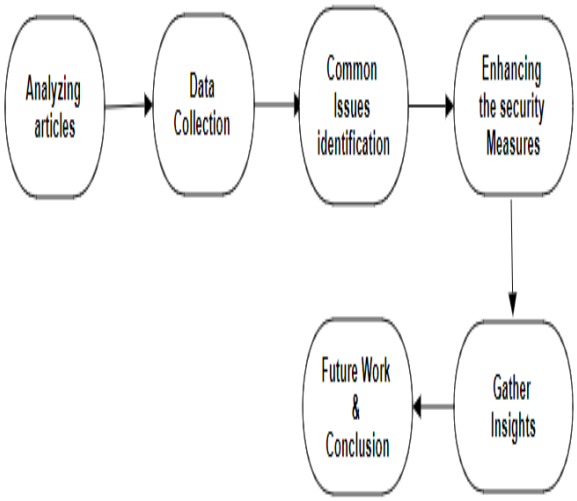

Fig2 Steps

- **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 [5] [6], and recent studies on distributed trust protocols [7].

4. Implementation Details

Following are the implementation techniques/details that are to be used to finish all the research gaps.

Choosing Suitable Distributed Protocol:

The most suitable Distributed Protocol that we chose was proposed by [2]. It focuses on the improvement of security and trust protocols in IaaS environments. It was chosen because it

tended to handle the trust and security issues described above in Section 2.

Design and Architecture:

The architecture that is to be used is decentralized. The architecture includes the 2 following important components:

- **Trust Evaluation:**

  These nodes will be responsible for evaluating and synchronizing the security and trustworthiness of the customers and cloud service providers.

- **BlockChain Integration:**

  For secure and transparent security and trust protocol, blockchain technology is utilized.

Programming Language and Storage:

Using Python as a programming language due to its versatility and ease of use in the IaaS cloud environment.

Moreover, for decentralized storage purposes, distributed storage solutions Such as IPFS (or any other) are used for securing and storing sensitive and trust-related data.

API integration and Identity and Access Management:

Development of API for easy and good-quality interaction between distributed trust protocol and IaaS cloud providers.

Furthermore, the policies of IAM (Identity and Access Management) are to be utilized to control access based on trust scores and different thresholds.

Scalability and Interoperability:

To handle large-scale trust evaluation, different sharding, and off-chain processing techniques are used.

Standard APIs are used to ensure high-quality interoperability.

Data Encryption and BlockChain:

Firstly, end-to-end encryption is to be implemented to ensure high security and improvement of trust protocols.

Secondly, permissioned blockchain is utilized to handle access to the data stored on the IaaS cloud.

Testing:

Conducting user accessibility tests to assess the usage of the user with the trust protocols.

After conducting testing, enhancing the trust protocols and security measures based on the results and reviews of the users, thus improving the trust mechanisms while maintaining transparency.

5. Expected Results Obtained

Following are some of the changes that are expected after the implementation of the above-discussed architecture.

Improve Trust Evaluation Accuracy:

After utilizing a decentralized mechanism, the trust protocols should show improved security and trust protocols which should be reliable and trustworthy as well.

Decrease in Trust Violations:

The events of trust violations like unauthorized access, hacking, and leaking of sensitive data should be minimal. Following are the highlighted parts of the world where trust violations

are maximum i.e. maximum complaints regarding trust protocols

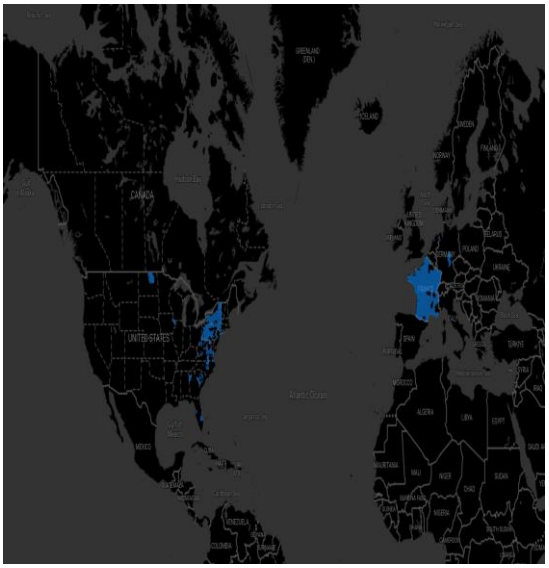

Fig3 Maximum trust violations

Enhanced Transparency:

After the use of distributed trust protocol with blockchain technology, transparency is expected to be improved, enhancing the trust of the IaaS users on the cloud and its providers.

Data Integrity:

The usage of distribution trust protocol is to ensure the confidentiality and security of the user's data stored on a cloud through different secure storage mechanisms and cryptography techniques.

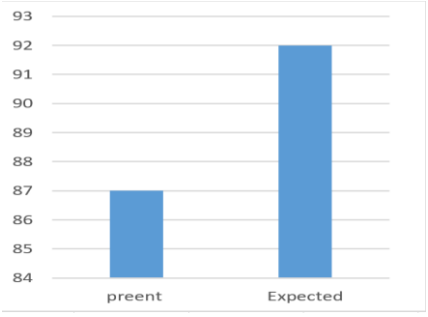

Fig4 Data Integrity Present Vs Expected

User Experience Enhancement:

The cloud providers made the IaaS cloud easy to use for the users/customers. By integrating different mechanisms, the users can now use and experience the secured environment for storing their data. Decentralized storage was used for this purpose.

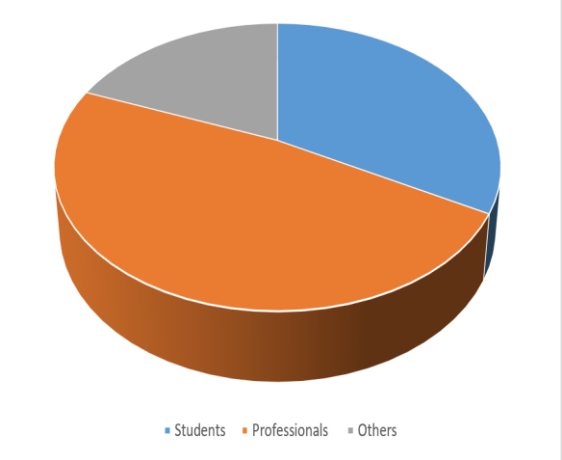

Fig5 Different Categories' Experience Enhancement

Throughput and Latency:

Evaluate the protocol's throughput and latency, ensuring that trust evaluations are performed efficiently without introducing significant overhead.

6. Conclusion and Future Directions

As a part of our research, we utilized the Distributed Trust Protocol (DTP) to tackle security and trust concerns in Infrastructure as a Service (IaaS) computing. Our study highlighted the significance of decentralized methods like DTP in strengthening trust evaluation mechanisms within cloud environments.

We were able to showcase the effectiveness of our approach by improving the accuracy of trust

evaluation, minimizing violations, and strengthening user privacy in IaaS. In the future, we suggest researchers concentrate on enhancing the scalability and real-world deployment of the DTP, integrating it with emerging technologies, and further improving user experience.

Our advancements in distributed trust protocols for IaaS contribute to the development of secure and trustworthy cloud environments. This fosters industry adoption and addresses evolving security challenges.

Real-World Deployment and Evaluation:

Conduct a comprehensive evaluation of the DTP in real-world IaaS scenarios to assess its effectiveness, performance, and user acceptance. Evaluate system throughput, latency, and overall trustworthiness under operational conditions.

Integration with Emerging Technologies:

To ensure secure interactions across nodes & devices in distributed cloud infrastructures, consider integrating DTP with edge computing & IoT. This enhances security, confidentiality & privacy, protecting data from unauthorized access or modifications.

Standardization and Adoption:

Collaborate with industry stakeholders to promote DTP adoption as a standardized framework for distributed trust in IaaS computing. Contribute to industry standards and best practices to foster interoperability and widespread adoption across cloud providers.

7. References

[1] Pascal M.Mutuli , “A Multi Tendance Cloud Trust Model using Quality of Service Monitoring: A case of Infrastructure as a Service”, 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

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

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

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