Title: Enhancing Data Security in Cloud Computing through Homomorphic Encryption

Introduction:

Cloud computing has emerged as a transformative paradigm in the field of Information Technology (IT), offering scalable resources and services to users over the internet. This technology has revolutionized how organizations store, process, and manage data, resulting in increased efficiency and flexibility. However, concerns over data security and privacy have also grown due to the centralization of data in cloud environments. In this context, homomorphic encryption presents a promising approach to address the security challenges associated with cloud computing. This research aims to explore the feasibility and effectiveness of utilizing homomorphic encryption techniques to enhance data security in cloud computing, particularly in the realm of Information Technology.

As cloud computing continues to gain traction, the security of sensitive data stored and processed in cloud environments becomes a paramount concern. Traditional encryption methods provide a level of protection but necessitate data decryption for meaningful processing, introducing potential vulnerabilities during the data's lifecycle (Gentry, 2009). Homomorphic encryption, a cryptographic technique that enables computations to be performed on encrypted data without decrypting it, offers a potential solution to this challenge (van Dijk et al., 2010). By preserving the confidentiality of data while allowing computations, homomorphic encryption holds the promise of safeguarding sensitive information in cloud-based IT systems.

The literature demonstrates the significance of incorporating homomorphic encryption in cloud computing for improved data security. Research has shown that homomorphic encryption can be applied to various IT scenarios, such as secure data sharing and processing in the cloud, while preserving the privacy of sensitive information (Naveed et al., 2015). Moreover, studies have highlighted the practicality and feasibility of implementing homomorphic encryption in real-world applications, thereby dispelling initial concerns about its performance overhead (Halevi & Shoup, 2014).

Through this research, we intend to delve into the practical implications of employing homomorphic encryption within the IT domain to enhance data security in cloud computing. By conducting a comprehensive analysis of the benefits, challenges, and potential trade-offs associated with this approach, we aim to contribute to a deeper understanding of the role that homomorphic encryption can play in safeguarding sensitive data while still enabling efficient computation in cloud-based IT systems.

References:

Gentry, C. (2009). A fully homomorphic encryption scheme. PhD thesis, Stanford University.

van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V., & Wichs, D. (2010). Fully homomorphic encryption over the integers. In Advances in Cryptology – EUROCRYPT 2010 (pp. 24-43). Springer.

Naveed, M., Prabhakaran, M., & Gunter, C. A. (2015). Dynamic searchable symmetric encryption. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 965-976).

Halevi, S., & Shoup, V. (2014). Algorithms in helib. In Advances in Cryptology – EUROCRYPT 2014 (pp. 554-571). Springer.

Github link

<https://github.com/UdaraAravinda98>