COS 720 Project

Name: Nathan Opperman
Student No: u21553832

March 21, 2024

1 Research Overview

Some of the more recent developments of Cloud Computing Security is the adoption of Zero Trust cybersecurity paradigms. This is because in Cloud Computing network location is no longer a factor in the security of resources and so permitter security is not viable. According to [2], Zero Trust Architecture (ZTA) emphasizes a principle of 'never trust, always verify,' shifting the security paradigm from perimeter-based trust assumptions to a model where no user/entity is implicitly trusted regardless of their location on the network and must always be continuously verified. Another important development is the use of micro-segmentation where the network is divided into smaller segments where access is restricted between them. According to [1] this mitigates the spread of threats/damage across the network. One development specific to data privacy has been the use of homomorphic encryption of sensitive data which allows computations of encrypted data without decrypting it.

Cloud Computing Security entails guaranteeing the confidentiality, integrity and availability of data and applications in the cloud though techniques and procedures that are independent of the physical infrastructures location(s) and other users of said cloud resources.

References

[1] S.-H. Joo et al. Strengthening enterprise security through the adoption of zero trust architecture - a focus on micro-segmentation approach -. *Journal of Information and Security*, 2023.

[2] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. NIST special publication 800-207: Zero Trust Architecture. Technical report, National Institute of Standards and Technology (NIST), Advanced Network Technologies Division, Information Technology Laboratory, August 2020.