Extended Research Abstract:
Database technologies and data models for cloud computing

Cybersecurity in Cloud computing

Cloud computing is becoming the default data and database storage method for companies both large and small, mainly due to the benefits of outsourcing computing power, data storage and cyber security. Cyber security has become increasingly more important especially after GDPR, as a result datacentres for cloud computing have had to try and solve solutions relating to the confidentiality of data and the auditability of the security.

The reason that the cyber security of databases in relation to cloud computing was chosen is that as part of Computer Science cyber security was a module. As a result I have a basic knowledge that this research can build on in terms of cyber security. As for the cloud computing element, in Year 1 system architecture was heavily discussed as well as how datacentres work.

The way that cyber security with in regard to cloud computing works is that the datacentre has to provide the cyber security for their clients. The datacentre providers have to achieve two goals, confidentiality of data and auditability of the cyber security measures. The ways that confidentiality is normally done is by using protocols which are designed to be unbreakable. Auditability however is done by using remote attestation methods. Remote attestation is normally done by using a secure module known as a trusted platform module to create a system summary which is impossible to forge as proof to the user of the systems' security. In a virtual environment like with cloud computing virtual machines can migrate from one location to another, this is normally done when a virtual machine is used and when it is not used. As a result the current methods of using trusted platform modules will not be enough to ensure the security of the data being ran on these virtual machines. As a result there are several methods being looked into such as machine learning tools to monitor cloud computing servers to detect changes to the hardware or data breaches and weird traffic flow. As well as this developing secure storage and transfer for virtual machines by ensuring that when the data is moved from one place to another a bot can be used to check the servers first and give the all clear.

The solution I went with is using something that is called a Private Virtual Infrastructure datacentre. The way that these work means that the risk of security breach is reduced for both the client and service provider. A bot finds storage for the data by pre-measuring the server for common security features such as a firewall etc, the both then gives the all clear and the data can be moved across. The bot however continues to monitor the security of the server as well as the overall security of the datacentre. This way the client retains control of their data.

In summary, cyber security in cloud computing has become more and more important especially due to the rise of legislation like GDPR. The best way to implement cyber security around data is still being discussed and new technology is always in the works, as can be seen current technology is now focusing on bots and machine learning to help provide cyber security for cloud data storage.

Bibliography

Chen, D., Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing, International Conference on Computer Science and Electronics Engineering, [online] pp. 647-651. Available at: https://www.researchgate.net/publication/254029141_Data_Security_and_Privacy_Protection_Issues_in_Cloud_Computing?enrichId=rgreq-8a3dcd2e2e5932a86656e5a8ffae96be-XXX&enrichSource=Y292ZXJQYWdlOzI1NDAyOTE0MTtBUzozMTIwMDM1MTg3NjMwMDhAMTQ1MTM5ODg0MzA5MQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf [Accessed 27 Apr. 2018].

Hashem, I., Yaqoob, I., Anuar, N., Mokhtar, S., Gani, A. and Ullah Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, [online] 47, pp.98-115. Available at: https://www.sciencedirect.com/science/article/pii/S0306437914001288 [Accessed 26 Apr. 2018].

Kaufman, L. (2009). Data Security in the World of Cloud Computing. IEEE Security & Privacy Magazine, [online] 7(4), pp.61-64. Available at: http://ieeexplore.ieee.org/abstract/document/5189563/ [Accessed 27 Apr. 2018].

Krautheim, J. (2009). Private Virtual Infrastructure for Cloud Computing. In: HotCloud '09. [online] San Diego: USENIX. Available at: https://www.usenix.org/legacy/event/hotcloud09/tech/full_papers/krautheim.pdf [Accessed 27 Apr. 2018].

Santos, N., Gummadi, K. and Rodrigues, R. (2009). Towards Trusted Cloud Computing. In: HotCloud '09. [online] San Diego: USENIX Association Berkeley. Available at: https://mpi-sws.org/~gummadi/papers/trusted_cloud.pdf [Accessed 27 Apr. 2018].

Zhang, Q., Cheng, L. and Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, [online] 1(1), pp.7-18. Available at: https://link.springer.com/article/10.1007/s13174-010-0007-6 [Accessed 27 Apr. 2017].