**Essay Question Preparation:**

There are a number of security considerations that a DBA is required to consider when implementing a database system. There are security elements that are standard to all systems and there are elements that a deployment specific.

The MoD use many database storage systems that are held within a vacuum or ‘air’ moat, that is to say that there is no external access to those systems other than from very specific machines that are off the network. Amazon use cloud based data storage for many of their database system.

Explain the security measures deployed or considered by the DBA which are common to both types of system, then outline the risks to the data each of the systems is exposed to and how a DBA could ensure that the security risk is minimised.

You are expected to use citations (Harvard style) and illustrations to support your points.

The following elements are expected to be included in the discussion:

• In the MoD system how is access gained to the database? How can a DBA use profiles and roles to limit access.

• The role of encryption in data storage

• The way databases use encryption to store database password can vary from DBMS to DBMS does that matter?

• Have Amazon ever had their data hacked and stolen? What does that tell you about the database security?

• What is the biggest weakness in any database security system? How should the DBA minimise the risks?

**Essay Answer**

**Introduction**

In this essay, I will be discussing the number of security concerns that a DBA is required to consider when implementing a database system. I will be using real-life examples such as the MoD’s vacuum moat database, as well as amazons cloud based storage and highlighting their advantages and disadvantages, as well as any relevant information pertaining them.

**Database Security**

Database security is one of the biggest issues surrounding data. Database security uses various information security protocols to protect databases from becoming compromised of integrity, confidentiality and also availability.

A few database risks include: malware attacks, which lead to unauthorised data manipulation, overloading of the system, as well as data corruption. Another risk is that of unauthorised user access and activity.

If a system is designed for easy access, security suffers as a result, and conversely if built to extremely high security measures, becomes difficult for the user to operate, as highlighted by Ross J Anderson: “Anderson's Rule means you cannot construct a database with scale, functionality and security because if you design a large system for ease of access it becomes insecure, while if you make it watertight it becomes impossible to use.” (Porter, 2009)

There are ways to protect this data, with methods such as access control, encryption, backups and authentication. With these methods one can ensure the right people access the data, it can only be read with the right encryption key and ensure data is not lost.

Systems such as cloud storage are particularly vulnerable to attack and being compromised if left inadequately protected.

**Database Access**

Each database contains a list of valid users that can access it through running applications to connect, usually via a username which would be defined within the database.

Generally, access control includes authentication (Checking the user is who they say they are), authorisation (granting the user access via confirmation) and audit (Security checks, activities that may have affected the system during a specific operation). (Stallings, 2015)

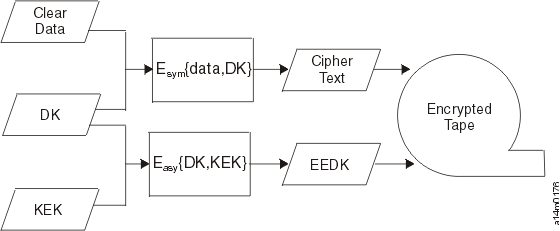
A DBA may choose one of the existing Access Control Models in order to restrict unauthorised access. Examples of these are Role-Based Access Control as well as Attribute-Based Access Control.

Defining specific roles and attributes is essential in restricting user influence and interaction over different aspects of the system, minimising data manipulation and unauthorised access. An example of this would be a shop in which the customers can view the data and stock, but only cashiers can manipulate the quantity of this, above them being a supervisor which can manipulate the price, and finally a manager which can further choose whether this product can be sold or not. Each user would have their own role and attributes assigned, in order to maximise protection.

**Encryption**

To protect sensitive data from attack or exposure, encryption would be used. Encryption is an old system (predating computers) but is effective and constantly improved to enhance security.

Two types of encryption algorithms can be used by the encryption key server: symmetric algorithms and asymmetric algorithms. Symmetric, or secret key encryption, uses a single key for both encryption and decryption. Symmetric key encryption is used for encrypting large amounts of data efficiently. (IBM, 2019)



**Why is this important?**

Encryption is vital to the security of sensitive data being transferred by using end-to-end protection by way of encryption and decryption from one site to another, meaning data intercepted would need to be decrypted by the attacker.

Encryption is used in many ways, one such example being passwords stored as hash symbols (which are obtained through different decryptions) within a database, meaning if stolen it would be difficult to reverse engineer a password hash to reveal the data. Encryption varies from system to system and DBMS’s are no exception.

If an attacker managed to crack the encryption of one system, and a second system shared the same encryption system, the attacker would also be able to get into this system.

This means having well developed encryption setups on your data is crucial to the security of databases.

**Cloud Storage**

Cloud storage is a system in which data is contained within ‘logical pools’ through a storage system that reaches across multiple servers. Typically, these are maintained through a hosting company. Cloud storage’s main task is keeping data readily available and accessible to users, whilst also ensuring the physical system is running and protected.

Cloud storage is typically accessed through cloud computing services, such as API (Application Programming Interface) and by applications that make use of these API’s, for example a CMS (Content Management System).

**Advantages:**

Advantages are as quoted: “Usability: Some cloud storage services may advertise desktop folders for Mac’s and PC’s. This allows users to drag and drop files between the cloud storage and their local storage. Bandwidth (Reduced bandwidth may be needed due to a lower amount of access), Accessibility ( Stored files can be accessed from anywhere via Internet connection), Disaster Recovery (Businesses that make use of cloud storage will be able to benefit from remote storage, which would allow for avoiding local damage to data) Cost Savings: Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.” (NT, 2014)

**Disadvantages:**

However, there are increased risks such as unauthorised access to physical parts of the system, the number of people accessing the system could be bribed or coerced into compromising the system. Another big issue in this regard is that by sharing the storage and networks, the cloud storage would require a WAN (Wide Area Network) in order to deliver on its availability, meaning that more security measures would need to be applied in order to protect this exposed network. An example of the type of security one could use would be a key-aggregate cryptosystem, which would alleviate business expense. (Chu, 2014)

**Amazon Data Breaches**

Amazon has suffered a few data breaches in recent years, such as in 2016 when over 83,000 user’s personal information, emails, passwords and use statistics were leaked in a hacking attempt. (ElevenPaths, 2016)

Another such breach occurred prior to ‘Black Friday’ of 2018, in which names and email addresses of user’s were leaked to the amazon website. (Brignall, 2018)

This tells us that database security is a critical issue that needs to be heavily considered and applied when handling big data such as Amazon. These breaches also indicate to us that encryption is not completely fool proof.

**Vacuum or ‘air’ moat**

Traditionally a moat is a defensive strategy designed to keep out attackers by surrounding the structure with water, and only accessible via one point. A vacuum or ‘air’ moat behaves in the same way. The database is isolated from all networks, and is only accessible via a singular machine, likely itself off-network for enhanced security.

The Ministry of Defence (MoD) uses this strategy to prevent outside attacks getting in, as data held by the MoD is likely vital to state security.

This has advantages, security being the biggest. It means that regardless of how proficient an attacker may be at decryption or finding back-doors into these systems, with the system itself being isolated, these problems go away. It is also likely that this system has secure user access controls.

However, the disadvantage to this is that data can only be accessed by one point, which would be likely be a physical machine connected to the system. Human error could also be an issue, with the system being in a vacuum, one may assume that the lack of access means there would be no need to enforce user access controls.

# Bibliography

Brignall, M., 2018. *This article is more than 8 months old Amazon hit with major data breach days before Black Friday.* [Online]   
Available at: https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday  
[Accessed 5 August 2019].

Chu, C.-K., 2014. *Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.* [Online]   
Available at: https://ieeexplore.ieee.org/document/6497048  
[Accessed 4 August 2019].

ElevenPaths, 2016. *Amazon Data Leak.* [Online]   
Available at: https://www.elevenpaths.com/wp-content/uploads/2016/08/CyberSecurity\_Shot\_Amazon\_v1\_0\_EN.pdf  
[Accessed 5 August 2019].

IBM, 2019. *About Encryption.* [Online]   
Available at: https://www.ibm.com/support/knowledgecenter/en/STPRH6/com.ibm.storage.drives.doc/top\_tscom\_reuse\_encryptoview\_keys.html  
[Accessed 3 August 2019].

NT, B., 2014. *5 advantages and disadvantages of using Cloud Storage.* [Online]   
Available at: https://bigdata-madesimple.com/5-advantages-and-disadvantages-of-cloud-storage/  
[Accessed 4 August 2019].

Porter, H., 2009. *Nine sacked for breaching core ID card database.* [Online]   
Available at: https://www.theguardian.com/commentisfree/henryporter/2009/aug/10/id-card-database-breach  
[Accessed 3 August 2019].

Stallings, W., 2015. *Computer Security: Principles and Practice.* 3rd ed. New York: Pearson Education.