Set 4 Cloud Computing End Sem

Sayam Kumar
S20180010158

Q-1 Top Risks in cloud computing

① Loss of governance → In cloud computing, there can't be clear use of SLAs to ensure security and unauthorized access can happen. The best security practice is set to SLA's before using cloud and provide a clear demarkation of security measure.

② Isolation Failure → There can be cases where multi-tenant or multi child based servers have failures in one of their chid processes. Involves failure of compute, memory routing. The best practice to avoid is to persistent backups and regular checks of compute/memory

③ Data Protection → Protecting the user's/clients data is most important in cloud computing. The attacker can find multiple ways to find/exploit paths for data leaks. The best practice is to use encryption and hash functions to store data.

④ Compliance Risk - The cloud computing devices must be compliant to follow local and best security protocols. Eg→ SOC2 security compliance. In public cloud, each server should have different/isolated set of rules to be governed over.

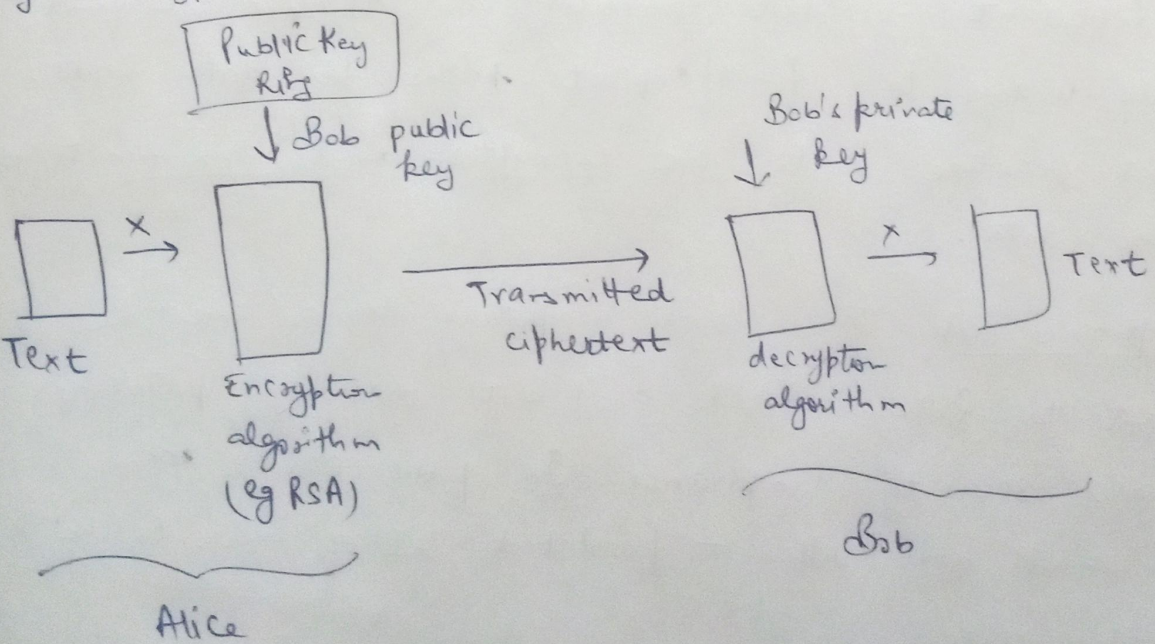
(5) Malicious Insider — There can be a case that a file on a single server is corrupt and in replicas, the same malicious file is copied. To avoid that in public cloud, scan the files for trojans, viruses etc.

Ans-2 Confidentiality and Authentication in Asymmetric Encryption.

In asymmetric encryption, there is a secret key made up of public and private key. Each user generates a pair of keys for encryption and decryption purposes.

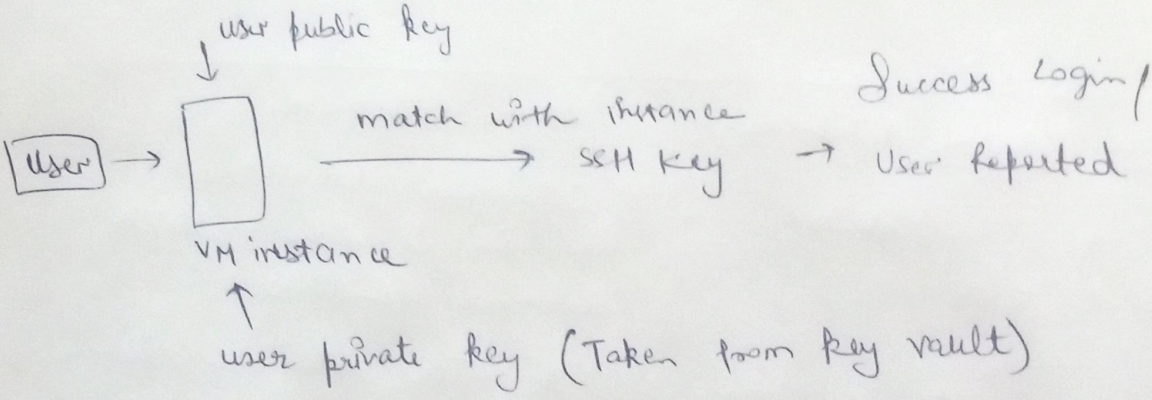
Confidentiality → data confidentiality is ensured by encrypting / decrypting of data at sender and receiver end respectively

Eg. Encryption with Public key Alice sending to Bob



Authentication → Asymmetric Encryption provides secure authentication using private keys. Eg→ Whenever we create a new VM, one private key is kept in cloud and its copy gets downloaded locally. With this way, there is a robust way to first identify a user first with a public key and then use private key for authentication.

Example of Azure



Ans 3 Two key shards A and B

A = follows normal distribution B = uniform dist

(a) Ranged sharding → In ranged sharding, the data must be uniformally spread over Range chunks for better efficiency. So, A option with normal distribution is better. Eg→ faster retrieval for queries like

$lt < x , or $gt > y

(b) Hashed Shards Hashed Sharding is used, then option B of uniform distribution is still better because hashed key are ideal with fields that change monotically / uniformly. It guarantees close to uni

(c) No, the above answers will not change from data distribution prespective. This is because once the data is stored either by ~~sh~~ range / hash shards, they are queried almost uniformly.

Answer 4 Relation database

(1) Here, it is an tabular, relational table.

(2) It stores data in rows

(3) Query optimization is less

(4) Follow data normalization rules

Eg- MySQL

Column database

(1) Columnar database has an id with multiple columnar familiar.

(2) It stores data in columns.

(3) Query optimization is better and thus have faster retrieval of data

(4) Can have ID with multiple columns

Eg- Apache Casandra, Hypertable, HBase etc.

Ans 4(b) Yes. There is a difference in NULL of SQL databases and schema agnostician in NoSQL databases. For these reasons -

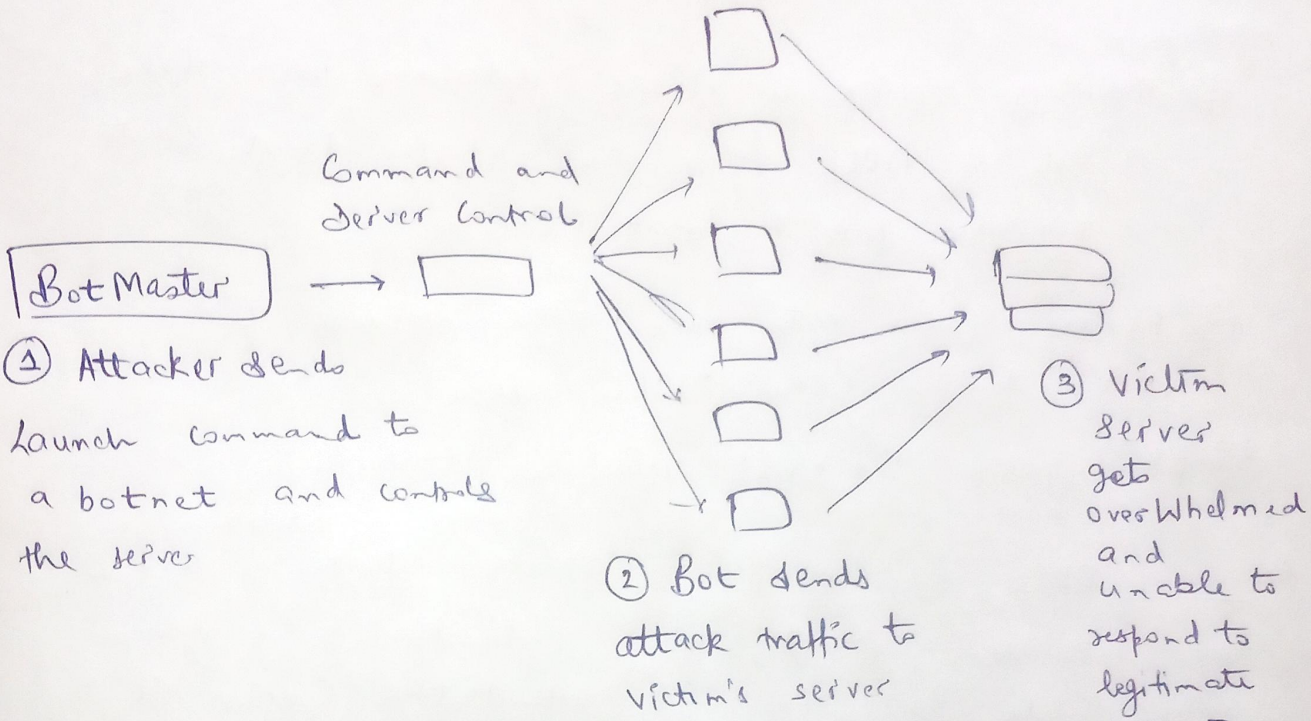
(1) Memory savings in NoSQL databases when there a lot of NULL values. We simply donot create a key-value pair/ document relation.

(2) Faster query rate in NoSQL because of not dealing with NULL values.

Simply, ignore the NULL values in database.

Answer 5 DDoS is denial of service attack in which the intruder aims to make networks or machines unavailable to the ~~intd~~ intended users. It is accomplished by flooding the targeted machine with uncountable requests. D extra stands for distributed DoS where many machines send requests to users.

Diagram Next Page



→ Yes, if the distributed attack has enough capacity to send requests, then cloud data center can be met down and if data center is not secure enough.

Private → Yes, depending on security protocols led by the company, DDoS can affect the entire system (Hard)

Public → Yes, they are more prune to DDos. (Easy)

Community → Depends on security protocols led by Community or in shared resources (Harder than private)

Hybrid → Depends on security protocols