# Quiz 4

Information security can be viewed as including three functions (or confidentiality, integrity, & availability)

- Access control
    - **Who** can access a computer system/data rightfully
- Secure communications
    - Requires encryption (commonly recognized as the encryption algorithm)
- Protection of private data
    - limiting availability of date to authorized recipients
    - integrity checks on the data

environmental factors that effect the evolution of info security:

- Computing power available
    - moore's law
- Growing user base
- Sharing of info resources

Independent factors that drive the evolution of security considerations -> cloud computing :

- Performance
- Environment

Security concerns of cloud operating models

- Infrastructure as a Service (IaaS)
    - Users want to
        - ensure that hardware-level services (i.e. ports and drivers) are protected from other processes running on the same physical server
- Software as a Service (SaaS)
    - Users want to
        - ensure that their data is protected from other users
        - Users data may need encryption to halt unauthorized access
- Platform as a Service (PaaS)
    - Users want to
        - ensure that platform services can be trusted
        - no man-in-the-middle attack

Passwords - a standard access control method & susceptible to brute-force hacking.

trade off between the security of the encrypted info & efficiency of the system

- ( boundary conditions: lifetime/value).

tradeoffs between efficiency & security

- apply to the storage & computation.

Hardware Security Models (HSM) - a computing device (physical) acting as a safe to manage digital keys

- strong authentication
- crypto processing services.

.The integrity of shared data

- verified with digital signatures.

key elements of internet security:

- Private key encryption
- Secure hashing
- Public key encryption

symmetric encryption

- unique key for each pair of

communicators Asymmetric encryption

- uses a diff key to encrypt than to decrypt.
- Commonly used to exchange private keys used by symmetric encryption

Hashing - an info security technique to mark a message to prevent tampering

Challenges of Using Standard Secruity Algorithms : lack of an indentifiable boundary

- Side channel attacks
- IoT ( internet of things)
- Backward compatibility versus security breach updates
- Hardware dependent

Some suggested security practices for cloud computing

1. Continous Monitoring:
    a. unexpected usage patterns
    b. changes in cloud resources
2. Sontring access control
3. Damage controls:
    a. Mitigation strategies : an alternative control and command network/ shutting down infected servers
4. Attack Surface Management
    a. access points exposed to an unauthorized user.
5. No residual footprints

Blockchain for security :block ,chain ,distributed ledger (i.e. crypto)

3 types of online business models

- B2B (Business to Business) - Dell ordering parts for a laptop

    - Godiva
- C2C ( Consumer to consumer) - Facebook & Ebay
- B2C (Business to consumer) - Bookstores being online
    - Amazon

Multiparty cloud :

- Better security
- Low latency : a data center closer to the end users
    - serve customer requests w least possible delays
- Autonomy : migrating/keeping 1+ copies of data and programs in different clouds
- Less disaster prone : SLAs (service level agreements)
- Optimized roi :
    - clouds built differently -> diff types of services

HSMs

- clustered for high performance/availability

Electronic design automation (EDA)

- software methods/flows/tools/scripts
    - used for very large scale integration (VLSI)

Evolution of EDA over time

- 1970 - 1979 (nascent years) : hand crafted small n simple designs
- 1980 -1989 (roaring decade) : 1,000,000 transistor designs (includes:schematic entry,layout editing tools)
- 1990 - 1999 (growing up) : circuit simulation, logic synthesis, analysis tools, layout automation
- 2000-2009 (maturing) : 1 billion transistor designs using IP blocks & SoC products
- 2010 - present (predictable EDA) : hyper scale computing w/ few private cloud technologies

Instruction set design

- high level design decisions about fundamental contract: hardware + software

Instruction set architecture(ISA)

- machine level instructions that target architecture will support on its own.

Architectural simulation and analysis

- exploration of microarchitectural design parameters
- choices such as organization/size of CPU caches
    - Or how many arithmetic logic units (ALUs) need to operate

Clock cycle-accurate simulation

- functional & timing simulation of architectural design in order to define the performance within each clock cycle.

Logic simulation and synthesis

- step of logic simulation using gate level implementation (accurate time models)

Timing simulation and analysis

- check for timing violations for low level design implementation

Pre-silicon validation

- running software OS on model of a chip
    - before silicon is placed

and more…

Considerations for cloud computing adoption:

- Licensing of EDA tools
    - prohibit sharing a tool between different geographical sites
- Asking EDA vendors whether the cloud suppliers even want EDA tools in the cloud
- How the eda tools are offered to the end users
- Eda customers' demands
- Present day EDA tools were not designed with cloud computing in mind
- Information Security in the Cloud must be solved to the satisfaction of all the stakeholders in the EDA industry

Load Balancing

- efficiently managing incoming tasks across a group of servers
    - ensure optimal loading of machines4
    - Too many jobs running on server-> slows server down
    - Task can be storage/I/O bound, CPU bound, memory bound

Algorithm available for load balancing:

1. Round robin
    a. If all servers/jobs are similar,
        i. distribute incoming tasks across servers sequentially
2. Least Connections
    a. new request is sent to the machine with smallest # of users/customer connections
3. IP Hash
    a. Forecasts the type of future tasks/compute resources that a customer will demand.

Edge Computing

- Strategy for computing where data is collected
- Creates both fabulous operational capability opportunities and HUGE security problems
- allows IoT data to be gathered @ edge,
    - Doesnt send data back to data center.

## Analytics in the Cloud

3 V Model for describing big data (+2) :

- Volume (amount of data)
- Velocity (speed of data in and out)
- Variety (range of data types and sources)
- Veracity
    - Data quality can vary : impacts accurate analysis
- Variability
    - Inconsistency of datasets : hamper processes that handle/manage

Most common uses of data analytics in the cloud

- Social Media
- Tracking Preferences
- Keeping Record
- Tracking Products

advantage of data analytics in cloud

- entire datasets can be used (instead of smaller samples)
    - represent heterogeneity of big data set.

MapReduce

- possible solution for large datasets
    - splits inputs into independent chunks.

Hadoop

- open source software project for reliable/scalable computing.
- a framework that allows
- the distributed processing of huge datasets across clusters of computers

Amazon’e Elastic MapReduce

- webservice that uses hadoop for processing/handling huge # of data.
- I.e. Public cloud customers have been using EMR for data transformation, machine learning, financial analysis, bioinformatics projects, and more.

IOT driven analytics in cloud

- Internet of Things (IoT)
    - collects data from multitude of interconnected devices
    - Data stored and analyzed in a cloud.

- BIG numbers of IOT sensors have enabled the collection of vast quantity of data.
    - improve decision making
    - finding important trends

Machine Learning in a Public Cloud

- ML
    - activities, tools, techniques used to detect patterns/predict future behavior.
- ML based solutions
    - perform specific tasks w/o external instructions

3 types of ML algorithms

1. Supervised and semi supervised learning
    a. training data
        i. Contains inputs and desired outputs
2. Unsupervised learning
    a. given data only specifies
        i. input
        ii. no desired output
3. Reinforcement learning
    a. building an exact model is nearly impossible or not feasible
    b. used to make decisions
        i. goal : maximize rewards

Process of Cloud Migration

1. Finalize business purpose for migration
2. Evaluate migration costs
3. Choose cloud environment (single or multi-cloud)
4. Determine deployment model (IaaS, PaaS & SaaS)
5. Cloud partner with right architecture
6. Define baselines for performance
7. data-migration plan
8. Migrate applications
9. test to ensure no vulnerabilities exist