Quiz 1

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

Different companies are using the cloud in different ways but overall most companies store their most crucial data in the cloud. At this point, most companies are migrating all their data and work to the cloud. The cloud is very beneficial in terms of backups [easier to store on the cloud bc you have more backup]

Types of cloud - Public , Private, Hybrid

- Private - used by government agencies mainly and data that companies want to keep very secret
- Public - most companies place their data in the public cloud as its much mor efficient and cost effective then having a private cloud

Over time companies are shifting from data centers to the cloud more and more

Virtualization vs abstraction

Companies incorporate a combination of SaaS , IaaS, and PaaS

SaaS - software as a service

IaaS - infrastructure as a service

PaaS - platform as a service

Cloud computing trends and needs

Trends

1. Abstraction of network, storage, db, security, and computing infrastructure
2. A price model that is retail in its conception
3. Service-Level Agreements

Historical evolution

- Idea phase (early 1960s)
- Pre - cloud phase (cloud started becoming prevalent in 2006 so this era was basically the 1990s - 2006)

- Cloud phase (2006 and after)

How did the cloud come to be

Phase 1

- Large system called “mainframes” located in back rooms that were accessed via terminals, had no local data processing, and utilized card-punching systems with job control language (a scripting language for mainframes).

Phase 2 - 1980s

- Stand-alone personal computers that could be connected via a modem
- Users interacted on a one-to-one basis using a mouse, keyboard, and display terminal
- Self - contained computing device that received additional software via floppy disk
- Eventually resulted in laptops
- This phase transitioned from terminal-based, single user-single job to GUI - based, single- user multiple jobs.

Phase 3 - Mid 1990s

- Development of web browsers to access the world wide web.
- Foundations of connecting users via the internet
- Utilization of TCP/IP protocol to make large sets of unreliable resources produce a reliable output.

Names of cloud providers: Amazon Web Services, Microsoft Azure, Google Cloud, etc.

Each cloud providers has different benefits.

Datacenters

- There are all kinds of datacenters around the world. Including underwater data centers that Microsoft has created
- Data centers require a large landmass and need to be at locations that don’t have lots of natural disasters (california is a no go)
- College Station Data center name: FiberTown
- It is important to keep a data center cool and non dusty
- One security issue of data centers is that you don’t want your data near another companies data as whoever comes to check that data may snoop into yours so a lot of big companies have their own data centers.

Unforeseen impacts

- Companies need to distribute their data loads amongst different providers because they do not want to be locked to a specific vendor. This causes problems in the long run
- Wearables are increasing in popularity (Professor Lightfoot mentioned that the future is wearables during his first lecture) because of its use of the cloud.
- Zoom became very popular because it saved recorded meeting footage to the cloud which was above its time as many of its competitors did not utilize the cloud to their benefit (i.e. Cisco Webex & skype)

- Impacted the it and business industries in ways we could have never imaged. Way more data than we could ever imagine as been able to be stored and used due to the utilization of the cloud.
- Cybersecurity needs to be uptight because we no longer have local stores to store data if the public cloud is hacked millions more private information is leaked [the scale of things is much larger bc of how grand the cloud is] . Efforts in the cyber security sector have been increased

Quiz 2

Cloud Computing Characteristics/ Benefits

- On demand self service
- Broad network access
- Very elastic
- scalable

What are performance issues in cloud computing? (Reliability and performance issues and concerns)

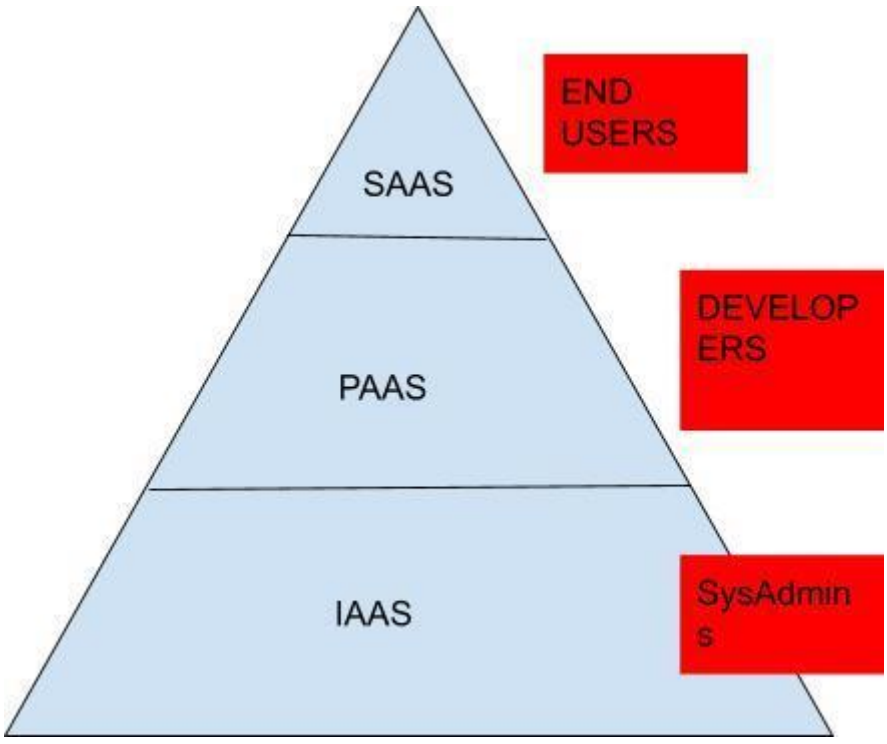
- Network latency
- Application processing delays
- Overall availability

- performance monitoring tools - help prevent potential problems.

Unforeseen Issues (cloud usage patterns , noisy neighbors) :

- Many companies tend to put their workload onto the cloud on the weekend when most of their employees are not in the office. This causes an excessive workload on the weekend compared to lets say wednesday (the middle of the workday week.
- Another issue is noisy neighbors. Noisy neighbors are neighbors that are using the same public cloud but are eating into your section of the cloud. This is problematic as it slows your automation and processing when your neighbor is taking most of the processing power.

The Cloud Computing Pyramid



At the top of the pyramid, we have S.A.A.S (Software as a Service) - They are also considered the end users. Examples of this include software like google doc, salesforce, and base camp. Software as a Service provides certain services that can fulfill a multitude of business needs.

At the middle of the pyramid, we have P.A.A.S (Platform as a Service) - They are also considered the developers. Examples of this include FORCE.COM and APP Engine. PaaS has a lot of similarities to IaaS. Its key difference is that its more advanced. For example, PaaS provides more than just infrastructure it also offers storage and cloud computing infrastructure combined with development tools that incorporate database management systems, Software development kits, and web servers. With all processes under one umbrella companies have a lower upfront software investment and have far less issues during testing and deployment

At the bottom of the pyramid we have IAAS (Infrastructure as a Service). Examples of this include AWS, Rackspace.com, and Go Grid. IAAS provides raw computing resources in a completely secured data center. The IAAS provides both hardware and software solutions that are ready to be used. In a majority of cases IAAS providers have the following features : data storage, managed development and/or hosting, pay as go options, easy scalability networking , and more.

Key differences of public, private, and hybrid cloud solutions:

- Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Different companies are using the cloud in different ways but overall most companies store their most crucial data in the cloud.
- At this point, most companies are migrating all their data and work to the cloud. The cloud is very beneficial in terms of backups [easier to store on the cloud bc you have more backup]
- Types of cloud - Public , Private, Hybrid
    - Private - used by government agencies mainly and data that companies want to keep very secret. The private cloud allows for more customization than the public cloud. With the private cloud we can use specified hardware with the specifications we need and this means less hardware cost and we aren’t paying for unutilized resources that we don’t actually need.a cloud infrastructure only for our dedicated customer or the organization so you can have a dedicated infrastructure for your clients or the organization and that would not be shared with the other users
    - Hybrid - hybrid cloud the hybrid cloud is basically the combination of the public and the private clocked it's based on the purpose and the requirements.during

high peak periods where workloads are much heavier it is best to switch to the hybrid cloud

- Public - most companies place their data in the public cloud as its much mor efficient and cost effective then having a private cloud. Public cloud has more sharing and syncing capabilities. It is more accessible and backing up data on the public cloud is much easier than on the private cloud.
  Over time companies are shifting from data centers to the cloud more and more Virtualization vs abstraction. Companies incorporate a combination of SaaS , IaaS, and PaaS.
  - SaaS - software as a service
  - IaaS - infrastructure as a service
  - PaaS - platform as a service Cloud computing trends and needs

1. Abstraction of network, storage, db, security, and computing infrastructure
2. A price model that is retail in its conception
3. Service-Level Agreements Historical evolution

History of the Cloud
- Idea phase (early 1960s)
- Pre - cloud phase (cloud started becoming prevalent in 2006 so this era was basically the 1990s - 2006)
- Cloud phase (2006 and after)

How did the cloud come to be?
Phase 1: Large system called “mainframes” located in back rooms that were accessed via terminals, had no local data processing, and utilized card-punching systems with job control language (a scripting language for mainframes).

Phase 2

- - 1980s
  - Stand-alone personal computers that could be connected via a modem
  - Users interacted on a one-to-one basis using a mouse, keyboard, and display terminal
  - Self - contained computing device that received additional software via floppy disk
  - Eventually resulted in laptops
  - This phase transitioned from terminal-based, single user-single job to GUI - based, single- user multiple jobs.

Phase 3
- Mid 1990s

● Development of web browsers to access the world wide web.
● Foundations of connecting users via the internet
● Utilization of TCP/IP protocol to make large sets of unreliable resources produce a reliable output.

Names of cloud providers: Amazon Web Services, Microsoft Azure, Google Cloud, etc.
Each cloud providers has different benefits.

Datacenters
- There are all kinds of datacenters around the world. Including underwater data centers that Microsoft has created
- Data centers require a large landmass and need to be at locations that don't have lots of natural disasters (california is a no go)
- College Station Data center name: FiberTown
- It is important to keep a data center cool and non dusty
- One security issue of data centers is that you don't want your data near another companies data as whoever comes to check that data may snoop into yours so a lot of big companies have their own data centers.

Unforeseen impacts - Companies need to distribute their data loads amongst different providers because they do not want to be locked to a specific vendor. This causes problems in the long run
- Wearables are increasing in popularity (Professor Lightfoot mentioned that the future is wearables during his first lecture) because of its use of the cloud.
- Zoom became very popular because it saved recorded meeting footage to the cloud which was above its time as many of its competitors did not utilize the cloud to their benefit (i.e. Cisco Webex & skype)
- Impacted the it and business industries in ways we could have never imaged. Way more data than we could ever imagine as been able to be stored and used due to the utilization of the cloud.
- Cybersecurity needs to be uptight because we no longer have local stores to store data if the public cloud is hacked millions more private information is leaked [the scale of things is much larger bc of how grand the cloud is] . Efforts in the cyber security sector have been increased

Quiz 3

Essential characteristics of cloud workload characterization

Workloads are grouped into four classes:

1. Rabbit - sensitive apps that perform better when not sharing cache
2. Turtle - Apps that do not really use their cache
3. Sheep - apps not perturbed by other apps
4. Devil - apps that do not like occupying cache and detrimentaly effect other apps

Workload categories can be split in two ways

1. Static architecture - implementation of solution architecture (i.e.parallel computational setup/big data storage)
2. Dynamic behavior - how resources are used in real time/stress that a workload places on the computational resources

Cloud Workload Categories

- **Slow communication** - minuscule amounts of info w/o a delivery time limit
- **Real-time local tasks** - hardware measurements given to a computer system
- **Location aware** - utilizing supplementary location input data to miniscule amounts of info w/o a delivery time limit
- **Real-time geographicaly dispersed task**s - multitude of scattered hardware measurements systems giving data to a network
- **Access control -** requests initiated by users where the response is to a different server with more authorized activity
- **Voice or Video over IP -** requests initiated by users where the response is through a server to each other
- **Big Streaming data workload category** - an interactive initiation followed by long periods of huge amounts of data sent to an end customer
- **Big Data storage workload category** - grand data (big datasets) which are periodically updated (requires a large download from time to time)
- **In-memory database workload category** - large # of data that is frequently & rapidly accessed
- **Many tiny tasks workload category** - independently running miniscule tasks
- **Tightly coupled intensive calculation workload category** - issues needing teraflops of computing power.
- **Separable calculation-intensive HPC workload -** enormous time-consuming # of calculations

- **Highly interactive multi-person jobs -** connectivity of jobs (i.e. discussion/ collaborating chats)
- **Single computer intensive jobs** - high speed substantial single-user taks that have lots of user interaction

- **Private local task** - traditional single user tasks

Computing Resources

- Persistent storage-
    1. user approximates a need
    2. gets a valid Service Level Agreement
    3. utilizes until Ithe resource requires an increase
- Compute power/computational capability
    - measured by:
        - CPU time/cycles
        - # & type of computer nodes available
        - # of cores available
        - the types and capabilities of CPUs assigned
- Network Bandwidth - examples that depend on network bandwidth
    - Xbox Live
    - Netflix
    - Playstation Network
- Broadcast transmission receivers -
    - need a special device added to the computer (i.e. GPS)
- Data busses within a server
    - CPU to memory
    - cache to main memory
    - memory to disk

Temporal Variability of Workloads

- two distinct cases in which the workload category would change.
    - When the job is incorrectly categorized
    - When the next step or phase of a job is a diff category than the current category

Essential characteristics of cloud management and monitoring

Cloud Management Terms

- Regions
    - Compromised of >= 2 availability zones
- Availability zones
    - A distinct location (inside a region) that won't be impacted by failures in other availability zones.
- Elastic load balancing
    - Automates process that distributes incoming app traffic across several EC2 instances

- Load balancers
    - Automatic scaling
    - Robust security
- Instance
    - Copy of an amazon machine image (AMI)
- Instance type
    - Specification that defines the cpu,memory,hourly cost, and storage capacity for a single instance
- Application performance

Cloud Management Requirements

- In-band
    - Agent that usually runs in a VM/OS
- Out of band
    - Monitoring tools that usually uses a baseboard management controller (has its own memory system + processor)
        - observing the main server's health metrics

Examples of Monitoring Tools

- Amazon Cloud Watch
    - a monitoring service for AWS resources and apps running on AWS
- New relic
    - App performance monitoring solution
        - uses agents placed in a VM - monitor how app is acting
- Nagios
    - a free & open source tool to monitor computer systems, networks, and infrastructure

Follow-ME cloud

- In reaction to the physical movement of a user's equipment : ability to seamlessly migrate a mobile user from 1 data center to another
    - NO disruption in the service
- Security Concerns
    - info leak issue during the transmission of the info/process after being stopped and before being freed up

Tradeoffs of freq vs infrequent monitoring of a server's performance

- frequent monitoring
    - can detect any variation of performance (even if it is a small one on CPU, network ,memory)
    - Frequent monitoring will however take more computational power
- infrequently monitoring
    - less computation intensive
    - User less likely to detect small variations in performance.

How to build a fail safe strategy :

- Always provide back up services
    - Back up data regularly
    - Host microservices independently
    - Improve intercloud compatibility
    - Eliminate single points of failure
    - Having hot swappable hard drives & backup power supplies

Metric to be monitored to ensure health of DC

- CPU, memory, and disk usage
    - Helps detect limited hard drive space, bandwidth , bottlenecks, high CPU utilization, and insufficient RAM
    - Efficient DC metrics : PUE (Power Usage Effectiveness), LEED (Leadership in Energy & Environmental Design) , PAR4, ASHRAE (The American Society of Heating, Refridgerating and Air Conditioning Engineers)

Key difference of peer to peer solutions

- difference between client server and peer to peer network:
    - Client - server : there is a dedicated server and specific clients in the client server network model
    - Peer to peer : in a peer to peer each node can act as both server and client vs in the client-server model , the server provides services to the client.

CAP Theorem

- CAP - consistency, availability, partition tolerance
    - Consistency - all clients simultaneously see same data.
    - Availability - system continues to operate (even when node failures are present)
    - Partition tolerance - system continues to operate (even when network failures are present)

Reliability and consequences of an outage

- cloud outage - a period of time in which a cloud providers services are unavailable to users.
- Reliability in cloud computing
    - Repetitive Redundant resources kick in automatically when the system experiences a issue/fault.

        - No downtime
- How to build a fail safe strategy
    - Always provide back up services
        - Back up data regularly
        - Host microservices independently
        - Improve intercloud compatibility
        - Eliminate single points of failure
        - Having hot swappable hard drives & backup power supplies

Miscellanious :

- Essential characteristics of cloud computing
    - On demand self service
    - Multi tenancy
    - Resource pooling
    - Broad network access
    - Rapid elasticity
    - measured service

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

Mualla Argin UIN : 728003004

Quiz 5

Future Trends

Cloud Computing future trends

1. Quantum computing
2. Edge computing
3. Secure Access Service Edge (SASE)
4. Cloud Regions
5. Green Cloud

Current limitations of cloud computing

1. Data movement
2. Perception of cloud security
3. Uncertain performance
4. Loss of control

Emergence of Internet of Things (IoT)

- Four basic communication models for IoT
    - Device to device
    - Device to gateway
    - Backend data sharing model
    - Device to cloud

emergence of machine learning

- Some use cases for IoT based machine learning
    - Point of Sales terminals
    - Consumer
    - Logistics
    - Point of Sales terminals
    - Utilities
    - Smart Home
    - Environmental Monitoring

Emergence of edge computing

- Self driving car

Security issues for edge computing

- Denial of service attacks
- Data theft
- Data integrity and falsification

- Invasion of privacy
- Identity authentication
- Unautorized access

- Activity monitoring

Solutions for edge computing security issues (step by step)

1. Monitor/track a threat
2. Identifying attackers
3. Attack recovery
4. Accidental and unintentional failures confused with security attacks

Example of IoT-based cloud service

- Fog computing - gathering and processing data at the local computing devices

A hardware root of trust has 4 basic blocks

- To run privileged software, a trusted execution environment (TEE)
- Software with special privileges that can, at the very least, provide cryptographic functions like the Advanced Encryption Standard (AES) code.
- a hash function to compare the currently executing code with the previously authenticated signatures of a trusted code binary as a form of tamper-proofing during boot and run time
- an application programming interface (API) or a straightforward user interface that allows users or higher-level applications access to the underlying hardware security features

Using these building blocks (above), hardware root of trusted can be created with :

- Secure cpu
- Security perimeter
- Secure data

Privacy-perserving multi-party analytics in a cloud

1. Anonymization
2. Secure Multiparty computation
3. Randomization

Outsorced computing using homomorphic encryption

- Homomorphic encryption
    - enables computations on ciphertext data by employing a type of encryption
- Applications of fully homomoprhic encryption
    - Client side encryption
    - Decentralized voting protocols
    - Private biometrics
    - Querying Encrypted Databases

Machine Learning for Secruirty

- Preventive Solutions
    - Multifactor authentication allows for the verification of login requests and incoming users.
- Corrective Solutions
    - It is possible to locate and eliminate phishing sites after identifying a pattern of attacks emanating from a specific set of IP addresses or geographic regions.
- Detective Solutions
    - by monitoring what happens in an account and pointing out any unusual transactions.Anti-spam detection can prevent incoming phishing emails.

Future Work Needed

- Interoperability between IoT devices and cloud

services Edge Computing

- A distributed computing paradigm known as edge computing brings data processing and storage closer to the data's sources.
    - will shorten response times
    - save bandwidth.
- 10 edge computing use case examples
    - Autonomous vehicles
    - Remote monitoring of assets in the oil and gas industry
    - Smart grid
    - Predictive maintenance
    - In hospital patient monitoring
    - Virtualized radio network and 5G
    - Cloud computing content delivery

- An architecture called fog computing uses edge devices to do a lot of computation/storage/communication locally and over the Internet backbone.
- Coined by cisco
- Examples
    - embedded application on a production line

A new category of edge or fog cloud computing is being created by combining locally intelligent devices with backend cloud-based processing. This new class of cloud computing offers novel usage models, but it also raises the possibility of new vulnerabilities and widespread cyber attacks.If vendors do not adhere to interoperability standards for their edge-based devices in proprietary cloud solutions, there are additional concerns regarding user lock-in.The rapid development of IoT-based solutions in the edge computing domain is currently held back by additional concerns regarding user data privacy and legal jurisdiction.In order to avoid any legal pitfalls, vendors and cloud service providers must discuss the policy framework with users.industry has wavered between huge focal PCs and restricted registering, bringing about half and half models adding to the winding utilization development.This currently requires

enormous focal PCs to deal with the circulated edge figuring interest.As networks become faster and machines become more intelligent enough to recognize data pattern patterns and make decisions, this trend is likely to continue.To ensure a level playing field for all players, it is essential to establish standards for the interoperability of computing devices at the edge and servers at the back end in this evolution.Hackers and security professionals are increasingly utilizing ML tools and techniques to advance their respective interests.

NIST/IEEE standards

- The Federal Chief Information Officer (CIO) has given the national institute of standards and technology (NIST) the responsibility of leading efforts to identify existing standards and guidelines in order to speed up the secure adoption of cloud computing by the federal government.
    - NIST collaborates closely with US industry, standard developers, other government agencies, and global standards leaders
        - to develop standards that will support secure cloud computing wherever standards are required.
- The USG Cloud Computing Technology Roadmap was created by the NIST cloud computing program in accordance with NIST's mission.
    - It is one of many support mechanisms for the US Government's (USG) secure and efficient adoption of the cloud computing model to cut costs and improve services.
    - Standards are essential for ensuring cost-effective and simple migration, meeting mission-critical requirements, and lowering the risk that significant investments will become technologically obsolete prematurely.In order to guarantee a level playing field in the global market, standards are essential.A memo from the White House emphasizes the significance of setting standards in close conjunction with private sector involvement.
- The existing standards landscape for interoperability, performance, portability, security, and accessibility has been surveyed by the NIST cloud computing standards roadmap working group.
    - These standards include models, studies, use cases, conformity assessment programs, etc.relevant to the use of the cloud.
- Cloud computing, according to the NIST definition,
    - a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources that can be quickly provisioned and released with little management effort or interaction from service providers..
- Numerous functions and requirements are already supported by cloud computing standards.Even though many of these standards were created to support technology that existed before cloud computing, like web services and the internet, they also support cloud computing's functions and requirements.

    - Specific cloud computing functions and requirements, such as virtualization, infrastructure management, service level agreements (SLAs), audits, and cloud-specific data handling, have been or are currently being supported by additional standards
- The NIST Cloud Computing aims to evaluate the current state of cloud computing-related standardization.
    - An inventory of cloud computing-related standards has been compiled by the Standards Roadmap Working Group.As needed, this inventory is being kept up to date.
    - Relevant standards for cloud computing have been mapped to the requirements of accessibility, interoperability, performance, portability, and security using the taxonomy created by the NIST Cloud Computing Reference Architecture and Taxonomy Working Group.
- Currently lacking in standardization are:
    - Functional interfaces for SaaS (Software as a Service)
    - Functional interfaces for PaaS (Platform as a Service)
    - business support
    - Provisioning
    - Configuration
    - Security
    - Self-service management interfaces for SaaS
    - Privacy

.

- a variety of Standards Developing Organizations (SDOs) are working on a rapidly evolving landscape of cloud computing-related standardization.
- Government organizations ought to likewise be urged to partake explicitly in distributed computing principles advancement projects that help the particular requirements and needs of their cloud registering administrations.

Recommendations regarding engagement between SDOs and federal agencies:

- **Recommendation 1** – Contribute Agency Requirements Agencies should coordinate and contribute clear and comprehensive user requirements for cloud computing standards projects.

- **Recommendation 2** – Participate in Standards Development

- **Recommendation 3** – Encourage Testing to Accelerate Technically Sound Standards-Based Deployments

- **Recommendation 4** – Specify Cloud Computing Standards

- **Recommendation 5** – USG-Wide Use of Cloud Computing Standards

Mualla Argin UIN : 728003004

NIST's primary function is to develop standards that organizations and government agencies can follow.

- enhance the security posture of private businesses and government agencies that handle government data.

When it comes to the NIST framework, the problem with these models is that

- NIST cannot really deal with shared responsibility.
- the framework assume a much more private method of operation than is becoming the norm in many industries.
- Longevity is a no no

Pros of NIST CyberSecurity Framework

- Unbiased and superior cybersecurity
- Long term risk management and cybersecurity
- Effects of ripples on supply chains and vendor lists
- Bridges business and technical stakeholders
- The framekwork's flexibility
- Built to meet future regulatory and compliance needs

Cons of NIST Cybersecurity framework

- Log files and audits have only 30 days of storage
- It cant deal with multiple third parties for cloud computing
- Compliance with Role Based Access System