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