**Members:**

**Autida, Griella Jane,**

**Cruzada, Joshua,**

**Orale, Jerimi, Quitoles,**

**Sheena Patrice.**

**Cloud Computing and Autonomic Computing: Pioneering the Future of IT**

**Objectives of the topic**

* Understand the concept and benefits of cloud computing.
* Explore the history and evolution of cloud computing and autonomic computing.
* Learn about different service models in cloud computing (IaaS, PaaS, SaaS).
* Examine the various applications and use cases of cloud computing and autonomic computing.
* Analyze the pros and cons of cloud computing and autonomic computing.
* Understand how cloud computing and autonomic computing works in different focus areas (personal use, business use, software development, big data analytics, IoT).
* Recognize the impact of cloud computing on data storage, software delivery, collaboration, and other aspects of technology.

**Scope of the topic:**

**What is Cloud Computing?**

Cloud Computing - Cloud computing refers to the delivery of computing resources, including servers, storage, databases, software, and networking, over the internet. It allows users to access and utilize these resources on-demand, without the need for on-site infrastructure or physical hardware. In cloud computing, data and applications are stored and managed in remote data centers, and users can access them from any device with an internet connection. This model offers scalability, flexibility, and cost efficiency, as users can easily scale resources up or down based on their needs and pay only for the resources they use.

**What is Autonomic Computing?**

Autonomic Computing - Autonomic Computing is a concept that refers to the design and development of computer systems capable of self-management and self-optimization without requiring significant human intervention. These systems are designed to continuously monitor and adapt to changes in their environment, automatically adjusting their behavior and configuration to optimize performance, reliability, and resource utilization. Autonomic Computing aims to reduce the complexity and management burden associated with operating and maintaining large-scale computer systems.

**History of Autonomic Computing**

Early 2000s: IBM proposes the concept of Autonomic Computing, drawing inspiration from the autonomic nervous system.

2001: IBM launches the Autonomic Computing Initiative, highlighting the need for self-managing computer systems.

2001-2005: IBM invests in research and development efforts to create autonomic capabilities in various areas, including self-healing, self-configuring, self-optimizing, and self-protecting systems.

2005: IBM introduces the Autonomic Computing Reference Architecture, providing a framework for designing and implementing autonomic systems.

2006: The Autonomic Computing Toolkit is released by IBM, offering tools and resources to develop autonomic applications.

2007: The Autonomic Computing Center of Excellence is established by IBM in collaboration with academia and industry partners to further research and development in Autonomic Computing.

2010s: Autonomic Computing principles and concepts continue to influence the design and development of computer systems, with advancements in areas such as cloud computing, network management, and cybersecurity.

Present: Autonomic Computing remains an ongoing area of research and development, with efforts focused on making computer systems more self-managing, adaptive, and efficient.

**C. Network Security**

AWS has outstanding network security as it has outstanding network configurations that are properly controlled and managed. The following are reasons for building AWS world-class network:

1. Secure Network Architecture

2. Secure Access Points

3. Transmission Protection

4. Amazon Corporate Segregation

5. Fault-Tolerant Design

6. Network Monitoring and Security

**D. Amazon S3**

A. Amazon S3 Amazon is one of the leading cloud computing providers and has the benefit of gaining customer trust in cloud computing. Amazon also recommended this trust by following safety standards. The following describes how Amazon maintained a good position during the security period in use. Amazon uses the Identity Access Management (IAM) framework to control access to its services. IAM is a framework used to identify, authenticate, and authorize users/users, processes/groups, or groups to access AWS resources. The framework supports a centralized view of user management, passwords, access keys, and policies. This configuration for AWS users, permissions, and services/services define which user can access the pre-defined authorized device. The framework works as follows:

1. When a user first registers with an email address and password, the account created is considered a root account with full access to all available resources and services in AWS. It is considered the best way to use IAM to build users, teams, and roles.
2. The created IAM user can be set to obtain a username, password, access key, and a set of access permissions for a specific account. IAM user roles are encouraged to ensure that no user can access all root account resources and verify the different login credentials for the assigned accounts.
3. The IAM group can be created based on daily activities or level of access. Those groups can be set to have a different set of access policies. It is recommended to set permissions based on user level not based on user level for better access management.

Setting access to the minimum access right is also recommended. With minimal rights, and to avoid the escalation of rights, the IAM Role can be used instead. IAM roles, unlike passwords or access keys, support the use of temporary security information. IAM policies are usually set to limit a particular source of access or time, based on other circumstances.

**References**

<https://www.ijraset.com/research-paper/aws-cloud-computing-technology#conclusion>

<https://resources.sei.cmu.edu/asset_files/technicalnote/2006_004_001_14666.pdf>