FEBRUARY EDITION

CHRIST
(DEEMED TO BE UNIVERSITY)
DELHI-NCR, INDIA

FINTECH :

THE FRONTIER OF FINANCE AND TECHNOLOGY

ISSUE NO. 6 VOLUME NO. 1

EDITOR'S MESSAGE

Dr. Mayank Kumar
Associate Professor
School of Business and Management

Greetings and welcome to Volume I Issue 6 of the Newsletter of Fintech Club of School of Business and Management, Christ (Deemed to be University, NCR Campus) – FINTECH- FRONTIER OF FINANCE AND TECHNOLOGY.

This newsletter is an initiative of the newly formed Fintech club which implores undergraduate students of SBM towards the latest Financial shifts which are influenced by the technology . The newsletter aims to act as a beacon of information on a monthly basis, contributed by the students of the Fintech club. Through this newsletter Fintech club is trying to bring the latest developments in the area of technology for financial firms to the readers and in turn this will try to fill the knowledge gap created by continuous evolution of technology in the financial sector.

CONTENTS

INFORMATION CENTRIC SECURITY

Information-centric security in cloud computing refers to a security approach that focuses on protecting the confidentiality, integrity, and availability of information stored and processed in the cloud. This security approach places information at the center of security considerations, rather than securing the infrastructure or network itself.

In this approach, security measures are applied to the information, such as encryption and access control, to ensure that only authorized users can access and use the information. Additionally, data protection policies and procedures, such as data backup and disaster recovery, are implemented to ensure that information remains available even in the event of a security breach or failure.

Information-centric security is important in cloud computing because the cloud infrastructure is often shared by multiple users and tenants, which can increase the risk of data breaches and unauthorized access. Additionally, because cloud computing involves storing and processing data remotely, it is important to ensure that the data is protected while in transit and at rest. Examples of information-centric security measures in cloud computing include data encryption, access control, data backup and disaster recovery, identity and access management, and threat detection and response. These measures help to ensure that sensitive and confidential information is protected and only accessible by authorized users.Overall, information-centric security in cloud computing is a critical aspect of securing data in the cloud and is necessary to protect sensitive and confidential information from unauthorized access and potential breaches.

OTHER KEY PRINCIPLES OF INFORMATION – CENTRIC SECURITY ARE :

- **Information must be protected throughout its life cycle whether it is at rest, in motion or at use.**
- **Information must be protected across all devices whether it being company managed, own device or any device of third party**
- **The information must be traceable**
- **IT and the owner of information should have dynamic control over security parameters.**

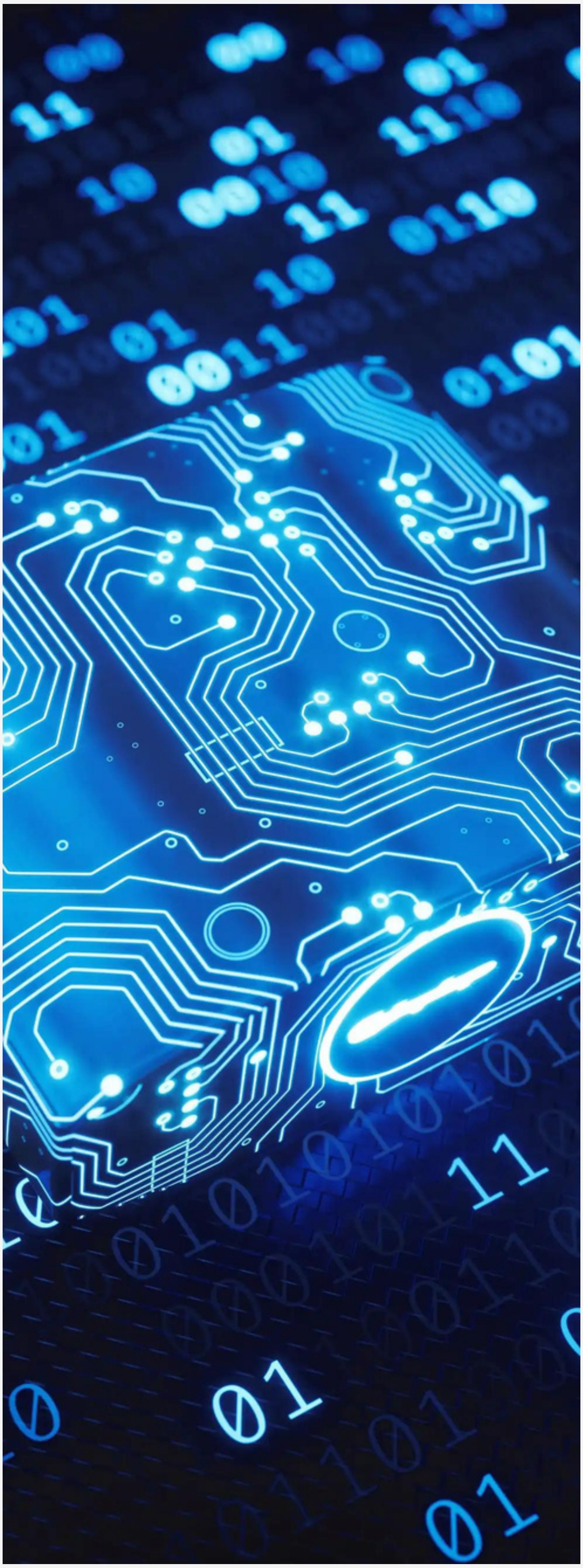
PRIVACY PRESERVING MODEL IN CLOUD COMPUTING

Everyone's perception of computer infrastructure, development processes, and software delivery have substantially changed as a result of the growing IT environment known as cloud computing. The next high-tech paradigm for the promise of tomorrow is expected to be cloud computing.The security of cloud computing has been examined in terms of its ability to maintain confidentiality, integrity, availability, accountability, and privacy.
Data processing security and data storage security are two components of safeguarding privacy in cloud systems.

Data processing security addresses the question of how to safeguard user privacy when it is being used in a virtualized cloud platform.
When data is kept in a data center, the issue of ensuring user data privacy is covered by data storage security.

The proposed privacy model has developed a triangular privacy preserving model [PPM].
A basic Cloud Computing: Privacy-Preserving Authentication Model. This architecture attempts to protect the accuracy of the data that the CU can access whenever needed and store in the cloud data center. The CU's capacity to adhere to the norms established and agreed upon by the CSP in the SLA is how this model assesses the CU's integrity. The TPA also verifies its own integrity (i.e., that it is not revealing the contents of the CU based on information gathered during the auditing process) and the services offered to the CU.

PRIVACY PRESERVING ARCHITECTURE



By protecting user data privacy, both internal and external attacks on the updated data are reduced in risk. The user interface, user engine, rule engine, and cloud database are the four primary elements of the architectural design.

1. ENCRYPTION TOOL

A customizable technique of access control can be presented that takes into account user privacy in a cloud setting. Each cloud user has several qualities associated with them that determine their access authority.A two-layer encryption scheme is used in this paradigm, with the base phase serving as the first tier and the surface phase serving as the second.

2.AUDITABILITY SCHEME

Auditing schemes lessen customer risk while also encouraging service providers to enhance their offerings. There are two types of auditability: private auditability and public auditability. You can get the best efficiency in the private auditability plan. Three components make up the data storage auditing method: the message authentication code (MAC), RSA-based holomorphic techniques, and Boneh-Lynn-Shacham signature (BLS)-based holomorphic methods.

IDENTITY MANAGEMENT IN CLOUD COMPUTING

FACT -: 80% of companies that adopt the cloud see improvements within their IT departments within six months.
These improvements were generally in the areas of efficiency, quality and security. Additionally, moving to the cloud helped these companies save money, cut costs and use staff more efficiently. After adopting the cloud, upwards of 90% of IT decision makers saw marked improvements in at least one area of the IT department.

Identity Management In Cloud Computing is the process of managing user identities and their associated access privileges. It is one of the components of Cloud security as it helps to ensure that only the right people have access to the right resources and because usernames and passwords are not that strong nowadays to protect organizations from data breaches. In simple words, it helps in restricting access to sensitive data.

Identity Management systems can be used to monitor user activity, create and enforce access policies, and protect against unauthorized access. It can also be used to automate user provisioning and deprovisioning.it reduces the time and effort required to manage user accounts.

Identity Management systems provide organizations with a secure and reliable way to manage user identities. By using these systems, organizations can easily comply with industry regulations. These systems also help the organization in managing user authentication and authorization.
There are several different types of Identity Management systems, including Single Sign-On(sso) systems, Directory services, and Identity and Access Management (IAM) systems. There are several different types of Identity Management systems, including Single Sign-On(sso) systems, Directory services, and Identity and Access Management (IAM) systems. The SSO system allows users to access multiple applications with a single set of credentials, while directory services provide a centralized repository for user information. It enables the user to access external resources . It also helps them to access internal resources.

Identity Management systems in Cloud Computing can be challenging as the organization must ensure that their Identity Management systems are secure and reliable . Additionally, organizations must ensure that their Identity Management systems are compliant with industry standards, also ensure that their system is able to scale as the organization grows and that they are able to adapt to changing user requirements. At last the organization must keep this in mind that their system is able to integrate with other systems and applications.

VIRTUALIZATION INFRASTRUCTURE IN CLOUD COMPUTING

Virtualization is a key component of modern Cloud Computing infrastructure. It refers to the creation of virtualized versions of physical hardware, such as servers, storage devices, and networks. This allows multiple Virtual Machines (VMs) to run on a single physical host, sharing its resources and providing greater flexibility, scalability, and cost savings.

Virtualization enables organizations to create an infrastructure that is highly flexible, scalable, and efficient. For example, it allows for the creation of Virtual Machines with specific configurations, such as operating systems, software, and network settings, that can be quickly and easily deployed. This makes it easier for organizations to deploy new applications, test new configurations, and manage their infrastructure more efficiently.

There are two main types of virtualizations :

- **Server virtualization and**
- **Network virtualization.**

Server virtualization allows organizations to run multiple Virtual Machines on a single physical server, each with its own operating system, software, and network settings. This can greatly increase the utilization of physical resources and reduce costs. Network virtualization, on the other hand, allows organizations to create virtualized network configurations, such as virtual switches, routers, and firewalls, that can be deployed and managed more efficiently than physical devices.

The benefits of Virtualization in Cloud Computing include increased flexibility, scalability, and cost savings. Virtual Machines can be quickly and easily deployed, and organizations can scale their infrastructure up or down as needed to meet changing demand. Additionally, Virtualization enables organizations to utilize their existing infrastructure more effectively, reducing the need for new hardware purchases.

In conclusion, Virtualization is a crucial component of modern cloud computing infrastructure. It provides organizations with greater flexibility, scalability, and cost savings, and enables them to manage their infrastructure more efficiently. By leveraging Virtualization, organizations can create a highly flexible, scalable, and efficient infrastructure that can meet their evolving needs.

DO YOU KNOW ?

- *Nearly one-half of US Government agencies use the cloud.*

Annually, these agencies spend $2 billion on creating, supporting and maintaining cloud services. Some experts say that the government is the largest user of the cloud in the world. Within the different branches of the government that use the cloud, commercial clouds, private clouds and shared clouds are all used. Private clouds, specifically, are employed by the government in an attempt to maintain security and control over the cloud.

- *The cloud computing market is projected to reach $106 billion by 2016.*

This represents a 30% growth rate from 2013. This is especially stark when you take into account that the entire enterprise IT industry is only expected to experience a 5% growth rate between 2013 and 2018.

TRUSTED COMPUTING

Trusted Computing is a concept in computer security that aims to enhance the security of computing devices and systems by utilizing cryptographic methods and hardware security mechanisms. The goal of Trusted Computing is to ensure that computing devices and systems operate as intended, free from attacks such as malware and data breaches. In this article, we will discuss the basics of Trusted Computing, its key components, and its applications.

Trusted Computing is based on the idea of creating a secure and trustworthy environment for computing devices and systems to operate in. This is achieved through the use of various technologies and approaches, including hardware security, secure boot, and trusted execution.

Hardware security is one of the key components of Trusted Computing

In this article, we will discuss the basics of Trusted Computing, its key components, and its applications.

Trusted Computing is based on the idea of creating a secure and trustworthy environment for computing devices and systems to operate in. This is achieved through the use of various technologies and approaches, including hardware security, secure boot, and trusted execution.

Hardware security is one of the key components of Trusted Computing. It is achieved through the use of Trusted Platform Modules (TPMs), which are dedicated security chips that are integrated into computing devices. TPMs can store encryption keys, passwords, and other sensitive information, and they can be used to ensure the authenticity and integrity of software and data.

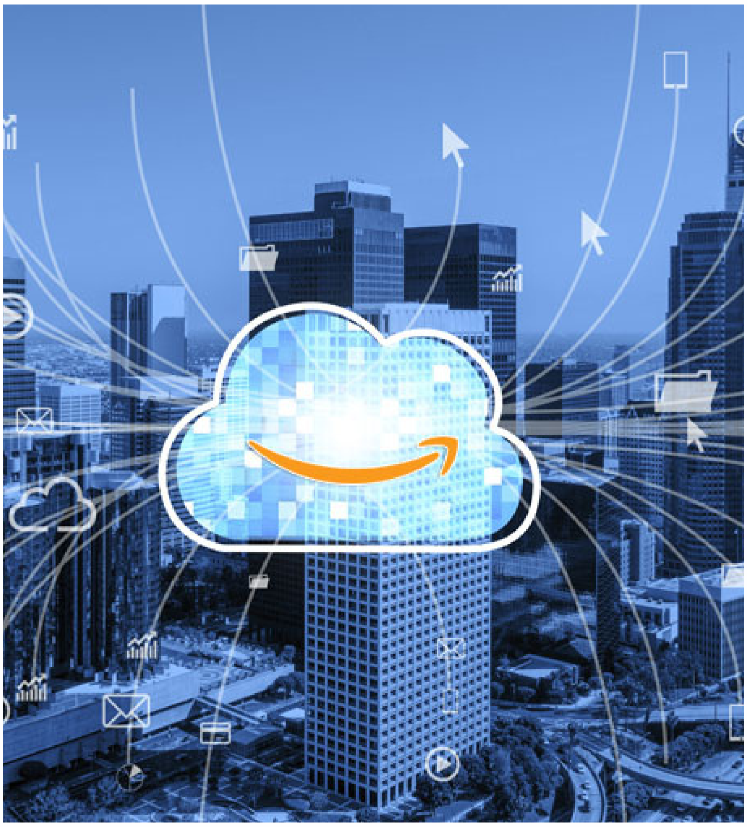
Secure boot is another important component of Trusted Computing. It is the process by which a computing device starts up and verifies the integrity of the operating system and other software before it is executed. This helps to ensure that the device only runs trusted software, and it helps to prevent attacks such as malware and rogue firmware.

Trusted execution is a technology that provides a secure environment for applications to run in, separate from the main operating system. This allows applications to run in a secure and isolated environment, protected from attacks and other threats. Trusted execution environments (TEEs) are often used in mobile devices and other computing systems to provide a secure environment for sensitive applications, such as financial transactions or data storage.

SOFTWARE PLATFORM

Cloud computing is a general term for anything including conveying facilitated administrations over the internet. Cloud computing works by empowering client devices to get information and cloud applications over the internet from remote physical servers, databases and the computer.

here are many issues in cloud computing which can be described as privacy, compliance, security, sustainability, Abuse, upkeeping of cloud, higher cost, recovery of lost data in contingencies, lack of resources, pay per use services charge and so on. So, to remove the issues the top cloud computing platforms are introduced which can be described: -



1) Amazon Web Administrations (AWS): -AWS provides different wide-ranging cloud IaaS administrations, which goes from virtual figure, stockpiling, and systems administration to finish processing stacks. AWS is notable for its capacity and register on request benefits, named as Versatile Figure Cloud (EC2) and Straightforward Capacity Administration (S3). EC2 offers adaptable virtual equipment to the end client which can be use as the base foundation for conveying processing frameworks on the cloud. It is probably going to look over an enormous assortment of virtual equipment designs including GPU and bunch cases. Either the AWS console, which is a wide-gone Online interface for recovering AWS administrations, or the web administrations Programming interface accessible for a few programming languages is

utilized to convey the EC2 cases. EC2 additionally offers the capacity of saving an unequivocal running occurrence as a picture, subsequently permitting clients to make their own layouts for sending framework. S3 is very much arranged into pails which contain objects that are put away in twofold structure and can be developed with ascribes.

2) Google App Engine: -Google App Engine is a versatile runtime climate much of the time devoted to executing web applications. These use advantages of the enormous registering framework of Google to powerfully scale according to the interest. AppEngine offers both a protected execution climate and an assortment of which improves on the turn of events of versatile and superior execution Web applications. These administrations include: in-memory reserving, versatile information store, work lines, informing, and corn errands.

3) Microsoft Azure: -Microsoft Azure is a Cloud working framework and a stage in which clients can foster the applications in the cloud. By and large, a versatile runtime climate for web applications and conveyed applications is given. Applications in Azure are coordinated around the reality of jobs, which distinguish a circulation unit for applications and express the application's rationale. Azure gives a bunch of extra administrations that supplement application execution like help for capacity, organizing, storing, content conveyance, and others.

4) Hadoop: -Apache Hadoop is an open-source system that is proper for handling huge informational indexes on ware equipment. Hadoop is an execution of MapReduce, an application programming model which is created by Google. This model gives two major activities to information handling: map and lessen. Yahoo! supporter of the Apache Hadoop project, and has invested extensive energy in changing the task to an endeavor to prepare a distributed computing stage for information handling. Right now, Hurray! Manages the world's biggest Hadoop bunch, which is additionally accessible to scholastic foundations.

5) Google Cloud: -Google cloud is a dependable, user-friendly, and secure cloud computing solution from one of the world's most powerful IT companies. Although Google Cloud's service offering isn't as extensive as Azure's, it's still sufficient to meet all of your IaaS and PaaS requirements. Its headlines include user-friendliness and security. Your first 12 months of service are also free, much like Azure. In addition, Google boasts that its services are less expensive and more budget-friendly than others.

6) IBM Cloud: -IBM Cloud is another cloud computing platform that focuses on IaaS (Infrastructure as a Service), SaaS (Software as a Service), and PaaS (Platform as a Service). It's one of the more cost-effective pricing plans on the market, and it's totally configurable, so you may save even more money. Using their APIs, creating an account is a breeze.

In the end, choosing the best public cloud provider is becoming a more sophisticated conversation that goes beyond size. The leading cloud computing firms are catering to a sizable and expanding market. As a result, they provide a wide range of cloud-related goods and services, such as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS).

ACCESS CONTROL

Access Control means that it is the ability of restricting access to information which is stored in the cloud. This enables businesses to ensure the security of their data and reduces risk.

Authentication mechanisms such as passwords, PINs, and multi-factor authentication are used to control access. Access Control can also be established at an organisation to authorise verified personnel to access company resources; authorisation to access can be restricted based on variables such as one's role, attributes, and more.

Types of Access Control

(1)Discretionary access control (DAC): The owner or administrator of the protected system, data, or resource determines who has access to it using this mechanism.

(2)Mandatory access control (MAC): People are given access in this nondiscretionary model based on an information clearance. According to various security levels, a centralised authority controls access privileges. In the military and government sectors, this model is prominent.

(3)Role-based access control (RBAC): RBAC gives access based on established business functions rather than the identification of the particular user. The idea is to give people access to only the data that is required for their positions within the company. This popular strategy is built on a complicated set of role assignments, authorizations, and permissions.

(4)Attribute-based access control (ABAC): Access is granted based on a collection of attributes and environmental conditions assigned to both users and resources, such as time of day and location.

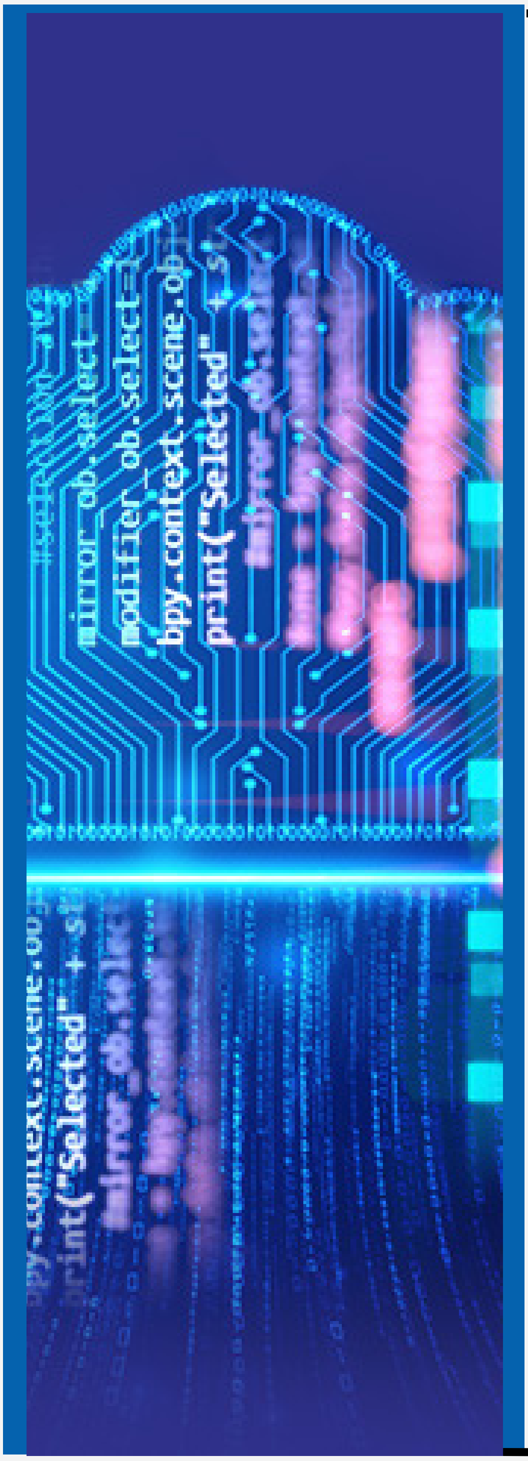
Types of Access Control

(1)Discretionary access control (DAC): The owner or administrator of the protected system, data, or resource determines who has access to it using this mechanism.

(2)Mandatory access control (MAC): People are given access in this nondiscretionary model based on an information clearance. According to various security levels, a centralised authority controls access privileges. In the military and government sectors, this model is prominent.

(3)Role-based access control (RBAC): RBAC gives access based on established business functions rather than the identification of the particular user. The idea is to give people access to only the data that is required for their positions within the company. This popular strategy is built on a complicated set of role assignments, authorizations, and permissions.

MEET THE TEAM



FACULTY COORDINATORS

DR. RUCHI PAYAL

DR. MAYANK KUMAR

STUDENT COORDINATORS

PRANJAL SINGH
6BBAFT | 20212644

BHUVANESWARI CH
4BBAFT | 21211424

EDITORS

ROHIT KUMAR
2BBAFT | 22211453

NITYA GOVIL
2BBAFT | 22211445