**INTRODUCTION**

* 1. **CLOUD COMPUTING**

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. A simple definition of cloud computing involves delivering different types of services over the Internet. From software and analytics to secure and safe data storage and networking resources, everything can be delivered via the cloud. You can access it from just about any computer that has internet access. cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. ... As long as an electronic device has access to the web, it has access to the data and the software programs to run it.

* 1. **TYPES OF CLOUD COMPUTING**

Cloud computing is a broad term which refers to a collection of services that offer businesses a cost-effective solution to increase their IT capacity and functionality. There are three main types of cloud environment, also known as cloud deployment models. The models are.

* Public cloud

A public cloud is a type of computing in which a service provider makes resources available to the public via the internet. ... Some public cloud providers offer resources for free, while clients pay for other resources by subscription or a pay-per-usage model. Public clouds are the most common type of cloud computing deployment. Microsoft Azure is an example of a public cloud. In a public cloud, you share the same hardware, storage and network devices with other organisations or cloud “tenants,” and you access services and manage your account using a web browser.

## Private cloud

## The private cloud is defined as computing services offered either over the Internet or a private internal network and only to select users instead of the general public. Also called an internal or corporate cloud, private cloud computing gives businesses many of the benefits of a [public cloud](https://azure.microsoft.com/en-in/overview/what-is-a-public-cloud/) - including self-service, scalability and elasticity - with the additional control and customisation available from dedicated resources over a computing infrastructure hosted on-premises. In addition, private clouds deliver a higher level of security and privacy through both company firewalls and internal hosting to ensure operations and sensitive data are not accessible to third-party providers.

## Hybrid cloud

## Hybrid cloud is a solution that combines a private cloud with one or more public cloud services, with proprietary software enabling communication between each distinct service. A hybrid cloud strategy provides businesses with greater flexibility by moving workloads between cloud solutions as needs and costs fluctuate. Hybrid cloud refers to a mixed computing, storage, and services environment made up of on-premises infrastructure, private cloud services, and a public cloud—such as Amazon Web Services (AWS) or Microsoft Azure—with orchestration among the various platforms

## There are three main service models of cloud computing. They are

#### IaaS (Infrastructure as Service)

This is the most common service model of cloud computing as it offers the fundamental infrastructure of virtual servers, network, operating systems and data storage drives. It allows for the flexibility, reliability and scalability that many businesses seek with the cloud, and removes the need for hardware in the office. This makes it ideal for small and medium sized organisations looking for a cost-effective IT solution to support business growth. IaaS is a fully outsourced pay-for-use service and is available as a public, private or hybrid infrastructure.

#### PaaS (Platform-as-a-Service)

This is where cloud computing providers deploy the infrastructure and software framework, but businesses can develop and run their own applications. Web applications can be created quickly and easily via PaaS, and the service is flexible and robust enough to support them. PaaS solutions are scalable and ideal for business environments where multiple developers are working on a single project. It is also handy for situations where an existing data source (such as CRM tool) needs to be leveraged.

#### SaaS (Software as a Service)

This cloud computing solution involves the deployment of software over the internet to various businesses who pay via subscription or a pay-per-use model. It is a valuable tool for CRM and for applications that need a lot of web or mobile access – such as mobile sales management software. SaaS is managed from a central location so businesses don’t have to worry about maintaining it themselves, and is ideal for short-term projects.

**1.2CLOUD STORAGE**

Cloud storage, one of the most basic services of IaaS, is a configurable data storage model that enables data owners to store their files in the cloud without retaining a local copy, which greatly reduces data owners’ storage and management burden of local files. Moreover, it is quite convenient for users to retrieve their files via terminals which have cloud access, such as mobile phones and tablet PCs. Cloud storage services have a number of significant advantages compared with traditional storage approaches, such as anytime and anywhere access, location-independent, on-demand services, flexible resources. Currently, an increasing number of individuals and enterprises are enjoying the convenience provided by cloud storage.

Cloud storage provides convenient, fast and unlimited capacity IT services to its users. However, due to the separation between data ownership and data management, cloud storage introduces some new data security challenges since data are hosted by cloud servers rather than data owners themselves. The cloud servers are not fully trusted. Any accidental data deletion by the cloud server, or worse, a physical catastrophe such as a fire or earthquake, might lead to permanent loss of users’ data. This is not exaggerating the dangers to frighten people. Symantec, a well-known information security company, reported a survey and showed that 43 percent of respondents experienced cloud data loss accidents and had to recover the data from backups.1 Thus, it is fair to claim that data integrity is the premise and basis of reliable cloud computing as well as big data analysis. If the integrity of cloud data is not ensured, the correctness of big data analysis and cloud computing cannot be guarantee.

**1.3 CLOUD DATA INTEGRITY**

In order to address the issue mentioned above, the concept of cloud data integrity auditing was presented, which can be mainly divided into two categories, namely Proof of Retrievability (PoR) and Provable Data Possession (PDP). PDP is a probabilistic detection protocol which employs randomly sampled data blocks rather than the entire file to perform cloud data integrity checking, which is more efficient than the deterministic auditing protocols, especially for large files. PoR protocols, similar to PDP, can not only detect the integrity of cloud data but also provide data retrievability.

**1.4 How to used?**

In order to reduce the complexity of certificate management in PKI, identity based (ID-based) cryptology was proposed by Shamir, in which the secret key binds with the user’s identity. Therefore, users can communicate without exchanging digital certifications. Due to the flexibility in key management, ID-based cryptology has been widely adopted in a variety of primitives, including in cloud data integrity auditing protocols. A number of ID-based cloud data auditing protocols have been proposed such as. The most commonly used identity information in existing ID based cloud data auditing protocols is an arbitrary bit string chosen by a user, such as names, IP and E-mail, which can be viewed as a text-based recognition related to the combinations of characters and numbers. With this identity information, one can register for a private key binding to his/her identity from the private key generation centre. There are three weaknesses when making use of ID-based protocols. First, identity might not be unique if identity information is not chosen properly. For example, the name “Nancy Helen” is probably not unique. Second, a user needs to “prove” to the private key generator centre that the claimed identities are indeed belong to him, which is typically verified by providing some additional documents such as one’s passport or identity card. However, these supplementary documents.

**1.5 LITERATURE SURVEY**

1. **Author**: Y. Deswarte, J. J. Quisquater, and A. Saidane,

**Title:** “Remote integrity checking,” Integrity and Internal Control in Information Systems.

**Description**: This paper analyses the problem of checking the integrity of files stored on remote servers. Since servers are prone to successful attacks by malicious hackers, the result of simple integrity checks run on the servers cannot be trusted. Conversely, downloading the files from the server to the verifying host is impractical. Two solutions are proposed, based on challenge-response protocols.

1. **Author:**John Green, David Marchette, Stephen Northcutt, Bill Ralph, **Title**: “Analysis Techniques for Detecting Coordinated Attacks and Probes”

**Description**: Coordinated attacks and probes have been observed against several networks that we protect. We describe some of these attacks and provide insight into how and why they are carried out. We also suggest hypotheses for some of the more puzzling probes. Methods for detecting these coordinated attacks are provided.

1. **Author**: J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong,

**Title**: “Privacy-preserving public auditing protocol for low performance end devices in cloud,”

**Description**: Cloud storage provides tremendous storage resources for both individual and enterprise users. In a cloud storage system, the data owned by a user are no longer possessed locally. Hence, it is not competent to ensure the integrity of the outsourced data using traditional data integrity checking methods. A privacy-preserving public auditing protocol allows a third-party auditor to check the integrity of the outsourced data on behalf of the users without violating the privacy of the data. However, existing privacy-preserving public auditing protocols assume that the end devices of users are powerful enough to compute all costly operations in real time when the data to be outsourced are given. In fact, the end devices may also be those with low computation capabilities. In this paper, we propose two lightweight privacy-preserving public auditing protocols. Our protocols are based on online/offline signatures, by which an end device only needs to perform lightweight computations when a file to be outsourced is available.

1. **Author**: Guangyang Yang, Jia Yu, Wenting Shen, Qianqian Su,

**Title**: [Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability](https://www.sciencedirect.com/science/article/pii/S016412121500268X) oud

**Description**: storage service has been widely adopted by diverse organizations, through which users can conveniently share data with others. For security consideration, previous public auditing schemes for shared cloud data concealed the identities of group members. However, the unconstrained identity anonymity will lead to a new problem, that is, a group member can maliciously modify shared data without being identified. Since uncontrolled malicious modifications may wreck the usability of the shared data, the identity traceability should also be retained in data sharing. In this paper, we propose an efficient public auditing solution that can preserve the identity privacy and the identity traceability for group members simultaneously. Specifically, we first design a new framework for data sharing in cloud, and formalize the definition of the public auditing scheme for shared cloud data supporting identity privacy.

**5.Author**: W Shen, [J Yu](https://scholar.google.com/citations?user=1hUwhuAAAAAJ&hl=en&scioq=Privacy-preserving+public+auditing+protocol+for+low-performance+end+devices+in+cloud&oi=sra), H Xia, [H Zhang](https://scholar.google.com/citations?user=irdGMlkAAAAJ&hl=en&scioq=Privacy-preserving+public+auditing+protocol+for+low-performance+end+devices+in+cloud&oi=sra), X Lu, R Hao

**Title**: light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium.

**Description**: verifies the integrity of cloud data, many cloud storage auditing schemes have been proposed. However, most of them incur a lot of computation overhead for users when data [authenticators](https://www.sciencedirect.com/topics/computer-science/authenticator) are generated or the data integrity is verified, which inevitably brings in heavy burdens to resource-constrained users. To overcome this problem, we propose a cloud storage auditing scheme for group users, which greatly reduces the computation burden on the user side. In our scheme, we introduce a Third Party Medium (TPM) to perform time-consuming operations on behalf of users. The TPM is in charge of generating authenticators for users and verifying data integrity on behalf of users. In order to protect the data privacy against the TPM, we blind data using simple operations in the phase of data uploading and data auditing. The user does not need to perform time-consuming decryption operations when using cloud data.