Chapter 19
Security Issues on Cloud Data Services

Nour Zawawi, Mohamed Hamdy El-Eliemy, Rania El-Gohary and Mohamed F. Tolba

Abstract In Cloud environments, resources are provided as services to endusers over the internet upon request. Resources' coordination in the Cloud enables users to reach their resources anywhere and anytime. Ensuring the security in Cloud environment plays an important role, as customers often store important information on Cloud storage services. These services are not always trusted by the data owners. Customers are wondering about the integrity and the availability of their data in the Cloud. Users need to save their data from outsider and insider attackers (i.e. attacker within service providers' coordination's). Moreover, any collateral damage or errors of Cloud services provider arises as a concern as well. Most of the vital security needs and issues regarding data Cloud services are mentioned in this chapter. The purpose of this chapter is to examine recent research related to data security and to address possible solutions. Research of employing uncommon security schemes into Cloud environments has received an increasing interest in the literature, although these schemes are neither mature nor rigid yet. This work aspires to promote the use of security protocols due to their ability to reduce security risks that affect users of data Cloud services.

N. Zawawi (✉) · M. H. El-Eliemy · R. El-Gohary · M. F. Tolba
Faculty of Computer and Information Sciences, Ain Shams University,
El-Kalifa Al Ma'mounst., Abbasyia, Cairo 11565, Egypt
e-mail: nourzawawi@gmail.com

M. H. El-Eliemy
e-mail: m.hamdy@cis.asu.edu.eg

R. El-Gohary
e-mail: dr.raniaelgohary@fcis.asu.edu.eg

M. F. Tolba
e-mail: fahmytolba@gmail.com

A. E. Hassanien et al. (eds.), *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, Intelligent Systems Reference Library 70,
DOI: 10.1007/978-3-662-43616-5_19, © Springer-Verlag Berlin Heidelberg 2014

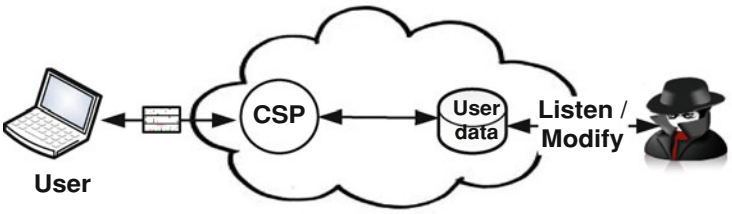

Fig. 19.1 Users' scenario for cloud environment

19.1 Introduction

In a public Cloud environment, resources and IT related capabilities are provided as services to the outer customers using the internet [1]. It depends on sharing information and computing resources instead of using local servers or personal devices to manage applications. It receives an increasing importance in commercial organizations. Moreover, it offers pay per use charge for the different required service. Essential characteristics of Cloud [1, 2] are on demand self service, broad network access, resource pooling, rapid elasticity, and measured service.

The prime revolutionary aspect of Cloud is its ability to deploy location independent services. At the same time, Service consumers (SCs) are no longer locked in with their providers. Cloud services take full advantage of the service oriented paradigm with a focus on the key attributes of statelessness, low coupling, modularity, and semantic interoperability [3, 4].

There are three, known types of Clouds: Infrastructure as a Service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). IaaS refers to the provision of virtualized hardware on which the client can run their operating system and software stack. In PaaS, the operating system and environment are provided and maintained for the client, who then runs their applications. In SaaS a Cloud Service Provider (CSP) runs and organizes the entire software system and provides software services [2].

Although users run their programs and applications depending on applications which have been physically deployed on their servers, reason for moving into Cloud computing is arising. It allows users to gain access applications from anywhere at any time through the internet. The CSP benefits are flexibility, disaster recovery, software updates automatically, pay per use model and cost reduction [5, 6].

Cloud computing still involves many risks concerning security, integrity, network dependency and centralization. Many security issues are considered based on the sensitivity and confidentiality of customers' data [6, 7]. Figure 19.1 represents the problems that prevent data owners of moving to depend on data services on the Cloud. The key issue of handling these challenges is empowering the trust between users and the service providers. Trust is the degree which clients will rely on for the assertions or security services provided by the cloud provider. Therefore, providing

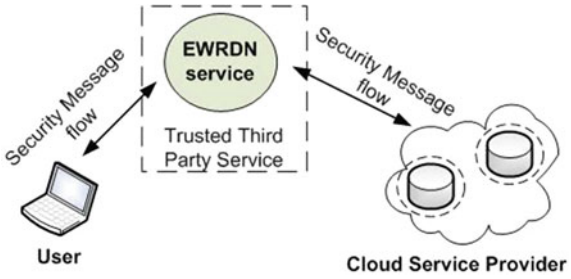

Fig. 19.2 EWRDN service proposed scenario

a trusted and secure data storage service in a public Cloud environment remains a challenge for service providers.

Availability, performance and security are the three main challenges when it comes to Cloud adoption. Nevertheless, performance needs to be measured according to time and space. In typical public cloud environments millions or even more simultaneous users are managed. This means that at full capacity, the system can handle these user and their data sets with minimal failures. The better an application's scalability, the more users it can handle simultaneously [8, 9]. Security in terms of integrity is the most important aspect of a Cloud environment. In this chapter, trusted security services which work against such security threats are illustrated. It achieves the missing trust enabling the parties in a Cloud environment to operate on their applications and services.

This chapter focuses more on the issues related to the data security and privacy aspects that may shape the trust in a public Cloud environment, such as data integrity, data confidentiality and service availability. As data and information will be shared with a third party, customers want to avoid unsafe service providers. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders has a critical importance. In previous work, several methods were proposed for securing data into the Cloud. This chapter discussed those methodologies and various techniques used to effectively and safely store data on the Cloud. An analysis for the advantages and drawbacks of those techniques is presented. Moreover, one discusses deeply the given aspects and criteria of one of the mature approaches that can handle efficiently these security issues. EWRDN service is [10] introduced as a trusted security service which tries to solve the previously mentioned scenario.

Figure 19.2 illustrates the proposed scenario of EWRDN service. EWRDN was built to be part of trusted third party service between user and CSP. EWRDN relies on changing the database schema by adding new columns. The function is used in constructing the new record as well as the secret key (K). In general, it combines some important features of database security and privacy like non repudiation, integrity, copyright protection and recovery. Moreover, it gives data owner more monitoring capabilities over their data. These features come from the missing trust between CSP and users.

EWRDN service uses watermarking techniques to prove if data has been tampered. By, saving data watermarks with users' original data. If the values match together, then data is tampered free. If not, then data owner has a legal evidence to prove that his data has been tampered with when it was at a CSP. Moreover, it provides a way to recover data, if unauthorized changes or errors happened. To the best of our knowledge, it is the first practical trusted Cloud privacy and copyright solution that solves previously mentioned lack of trust problems.

The rest of this chapter is organized as follows: Sect. 19.2 discusses the main security issues that affect in data over the Cloud. It has been divided into traditional and Cloud security challenges. It is followed by the main issues considered as the main security problems. Each section illustrates some of the recent research designed to overcome some security issues. Section 19.3 discusses data integrity over Cloud. Section 19.4 discusses data availability and Sect. 19.5 discusses data confidentiality. Section 19.6 illustrates the problems facing data security service over the Cloud with an introduction to a new service used to overcome the previous issues. Finally, Sect. 19.7 concludes the work discussed in this chapter.

19.2 Security Issues

Although CSP provides benefits to their clients, security risks play an important role resisting the development of any public cloud environment [11]. Users of online data sharing or network facilities are aware of the potential loss of privacy [12]. Protecting private and important information against attackers or malicious insiders is vital. So, an important question arises about the way to protect data from being exposed. In cloud scenarios there are three suspicious individuals for exposing data. They are:

- Cloud Service Provider (CSP)
- Internal Users
- Outsider Attacker

Therefore, how to save data from the three attackers is an important question that needs to be answered. Also, how to prove who has exposed data in order to take the related action needs to be answered. Moreover, there must be a well known technique to deal with data if errors or crashes appear.

Moving databases to large data centers involves many security challenges [9] such as accessibility vulnerability, and privacy. Also, there are control issues related to data accessed from a third party including data integrity, confidentiality, and data loss or theft.

In this section, one has categorized the main cloud security issues. This has been divided into two types; traditional and cloud (new) security challenges. Since, the common security challenges of traditional communication systems are inherited as well.

19.2.1 Traditional Security Challenges

Most businesses need some form of database security to protect confidential records and logical property from both external and internal threats. With violations of sensitive data, enhancement for security features appeared to upgrade the database security services. Consider a complete database security system to balance the security and privacy of your data with employee access. Developers recommend a database security model that sets controls to provide limited use. But because data needs to be stored, copied and made available instantly, database security remains a collaborative effort for companies.

Depending on your database security services database security measures can be set using various properties [13, 14]. They can be summarized as followed:

- Authorization: is finding out if the person, once identified, is permitted to have the resource. This is usually determined by finding out if that person is a part of a particular group, if that person has paid admission, or has a particular level of security clearance.
- Authentication: is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of signifying identity, such as a smart card, retina scan, voice recognition, or fingerprints.
- Confidentiality: it is the system policies that limits access or make restrictions on certain types of information. It could be explained as the way of protecting information from being exposed by unauthorized users. Organizations private data needed to be protected.
- Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. Where, it uses a digital signature to combine a public key with an identity. The certificate can be used to verify that a public key belongs to an individual. Also, it demonstrates the authenticity of a digital message or document.
- Encryption: is the process of transforming information (plaintext) using an algorithm (cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
- Integrity: refers to the consistency and accuracy of the data stored in a database. Data Integrity is based on how much accuracy of data, dependability of information and protection from unauthorized modification is required. Data only counts when it is correct, while tampered data prove to be costly.
- Backups: refers to the copying and archiving of computer data so it may be used to restore the original data after a data loss event. Backups have two distinct purposes: (1) Recover data after its loss where it is data deletion or corruption. Data loss can be a common experience of computer users. (2) Recover data from an earlier time, according to a user predefined data maintenance policy. It represents a simple form of disaster recovery, and should be part of a disaster recovery plan; in the same time backups should not be considered alone as a disaster recovery.

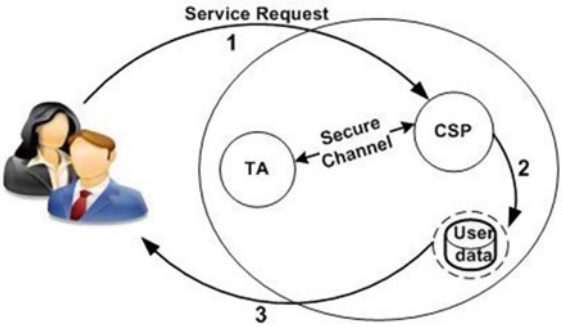

Fig. 19.3 Trust circle

19.2.1.1 Cloud Security Challenges

In order to, move data to the Cloud, data owner needs to trust CSP. So, trust circle is introduced in Fig. 19.3. It defines CSP identity adheres to by signing a business agreement, in order to support secure transactions among members. Also, it contains the way to access any service inside a public cloud environment. The circle of trust includes three parties. They are:

- Users who send requests into CSP coordination.
- Services which have effects on users' data.
- A third party service coordination which represents the Trusted Authority TA of all parties or participants.

The issues of establishing trust in the Cloud have been discussed severally in this chapter. Security and privacy are the two major concerns about using any of data exchange Cloud services. In the Cloud, virtualization lets user access computing power that exceeds that contained within their business infrastructure. To enter this virtual environment a user is required to transfer data throughout the Cloud [9]. It is concerned with protecting the confidentiality, integrity and availability of data regardless of the form the data may take [11].

There are currently many open problems in Cloud security that should be addressed by CSP in order to convince end users to use the technology. The most important concerns, in our view, are to guarantee that user data integrity and confidentiality are attained while they are stored in the Cloud systems. In a long, non transparent provider chain, it is difficult for an end user to even determine what security mechanisms are applied to data in the Cloud.

Other important security challenges are [9]:

- Loss of control, where users have no control over their private and personal data,
- Lack of trust (mechanisms), due to lack of Service Level Agreement (SLA) standards availability between users and providers,
- Multi-tenancy, which refers to a single instance of a software application serving multiple customers.

- Resources Location, end-users use the services provided by the CSP without knowing exactly where the resources for such services are located.
- System monitoring and logs, customers may request that CSP provide more monitoring and records for the customers' personnel data.
- Cloud standards, where standards are needed to achieve interoperability among clouds and to increase their strength and security.

There is number of key security elements that should be considered as an integral part of the Cloud application development and deployment process. In the meantime, there are a few technical issues like browser security, secure browser based authentication and Attacks on browser based Cloud authentication that needs to be built [15].

In the following, one presents a selection of security issues related to Cloud. Each issue has a major real-world measured impact [16].

- XML Signature: It is the way to save data against attacks for authentication or integrity. These types of attacks focus on the way to attack Simple Object Access Protocol (SOAP).
- Browser Security: The way to protect the users' computers. Since it used only for Input and Output. Also, it used for authentication and authorization of commands to the Cloud. So, CSPs need to develop some standards or a universal platform (standard Web browser).
- Cloud Integrity and Required Issues
- Flooding Attacks: The impact of such attacks is expected to be amplified drastically. This is due to the following types of attacks: direct and indirect denial of service

The next sections address three security factors that particularly affect Clouds, namely data integrity, confidentiality, and service availability.

19.3 Data Integrity

One of the most important issues related to trust and security risks is data integrity. Data is stored in the Cloud, as tuples, may suffer from damage during transition operations from or to the CSP. Moreover, data may be stored for several years. Data owners my do not have any mean to check if their data are similar to the form that they stored it initially. Customers are wondering about attacks on the integrity and the availability of their data in the Cloud from malicious insiders and outsiders, and from any collateral damage of Cloud services.

Cloud storage can be an attractive means of outsourcing the day to day management of data, but ultimately the responsibility and liability for that data falls on the company that owns the data, not the hosting provider. With this in mind, there are four points to understand

- The causes of data corruption,
- How much responsibility CSP holds,
- Best practices for utilizing Cloud storage safely,
- Methods and standards for monitoring the integrity of data.

The computing power to the Cloud environment is provided through a collection of data centers or cloud data storages (CDSs) present at different location and connected by high speed networks. With the emergence of cloud computing the CDSs is also emerging. The integrity within cloud storage consists of two techniques, integrity of data being transmitted from CDS and integrity of CDS. It faces an important issue that is security. Also, CDSs data integrity is an extremely important issue.

The work proposed by Rawat et al. [17] discusses the model based on Multi Agent Systems (MAS) architecture of Cloud and data encoding mechanism to enhance the integrity of CDSs. Where, MAS is used basically in artificial intelligence area for finding solution to the problems. It uses two agents in client side layer for data integrity. In Cloud they are used for developing architecture for data integrity at CDSs. Data encoding is one of the basic mechanisms of providing security. It combines MAS architecture for CDS and data encoding using hash values together to give a new mechanism. This can be done inserting a hash value concept in CDIBA agent of MAS architecture. CDIBA is responsible for the maintenance of cloud storage when data is entered into it, and if the data goes out of the cloud storage the hash values being used can be used to verify the data being transmitted is in correct format. Hence the complete process of reliable retrieval and reliable data transmission is guaranteed at the same time.

Motghare et al. [18] proposes a framework of data integrity. It uses Cooperative Provable data possession (CPDP). CPDP is a technique for ensuring the integrity of data in storage outsourcing. So, it addresses the construction of an efficient CPDP scheme and dynamic audit service for distributed Cloud storage as well verifying the integrity guarantee of an entrusted and outsourced storage which support the scalability of service and data migration. It offers two main contributions:

1. Efficiency and security: It is safer to rely on a public and private key encryption. In this every time parameters are generated and key exchange takes place this becomes more secure than symmetric and asymmetric algorithms. However, it is more efficient than the other techniques. Because it does not require lots of data encryption in outsourced and no additional posts on the symbol block, and the ratio is more secure.
2. Public verifiability: It provides public validation which allows users for information on the CSP has proved challenge(rewrite previous sentence). However, it is more efficient because it does not need the information for each block encryption.

Data corruption can happen at any level of storage and with any type of media. Bit rot (the weakening or loss of bits of data on storage media), controller failures, reduplication metadata corruption, and tape failures are all examples of different media types causing corruption. Metadata corruption can be the result of any of the vulnerabilities listed above, such as bit rot, but are also susceptible to software

glitches outside of hardware error rates. Unfortunately, a side effect of reduplication is that a corrupted file, block, or byte affects every associated piece of data tied to that metadata. The truth is that data corruption can happen anywhere within a storage environment. Data can become corrupted simply by migrating it to a different platform, i.e. sending your data to the Cloud. Cloud storage systems are still data centers, with hardware and software, and are still vulnerable to data corruption.

Based on the case studies proposed for home healthcare applications, one has chosen the following studies. They ensure data integrity on users' private data. Home Healthcare system is presented in [19], monitors, diagnoses and assists people outside of hospital setting. Specifically, it focuses on using TClouds on depressed patients. Establishing trust in the Cloud is a big challenge that requires collaborative efforts from academia and industry. It builds on the previous work [20]. Establishing trust is a fundamental requirement especially for Cloud's potential future as an Internet scale critical infrastructure. This requires the following: a. understanding and defining such services and their interdependencies, b. defining functions of the services which help in establishing their trustworthiness and c. building protocols and prototyping based on the defined functions. Specifically, it starts by developing the functions (e.g. LaaS, ACaaS, and PRaaS). In parallel, it establishes trust protocols based on the identified middleware functions. Once these are done home healthcare applications are deployed on the Clouds' platform architectures.

Current health cloud services offerings require full trust to CSP, where threats of malicious insiders have become one of the most dangerous attacks to protected data and applications in the Cloud. The work presented by Deng et al. [21] proposed a design for a trustworthy healthcare platform as a service. It is built on top of a trusted Cloud infrastructure that addresses technical issues and provides users with control over their personal data. Next to that, the platform addresses the needs to further decrease development and porting costs, while supporting rapid development of healthcare applications. The healthcare platform is proposed to host numerous healthcare applications, and also provide storage for medical data such as personal health records. The underlying trustworthy Cloud infrastructure is designed to increase the level of trust both for storage and computing. Various techniques are employed to provision security, data protection and resilience against data center outage and Cloud network failures. Two benchmark applications are implemented as a proof of concept to demonstrate features of the proposed the health platform. Where, it provides major benefits for both end users and service providers.

The other case one needs to discuss is Software as a Service (SaaS) applications. It exploits the potential of elastic Cloud infrastructures naturally are enabling new ubiquitous access scenarios for nomadic users, such as market salesmen and home healthcare medical assistants. SaaS applications typically require transferring data and resources to the Cloud infrastructure site. It raises several challenging issues spanning from access control to privacy protection of resources, ownership, and security of the data of the final SaaS users. However, although encryption of personal and enterprise data is strongly recommended by existing Cloud infrastructures typically they do not provide yet adequate encryption and key management support. Corradi [22] presented a real use case of home healthcare SaaS application deployed

on Amazon Web Service (AWS), and discusses the challenges and changes needed to add cryptography and key management capabilities to enable SaaS data protection. It shows experimental results that benchmark the new security functions over Amazon, demonstrating their applicability to SaaS production deployments.

The last case one discusses is the way to establish trust. Trust establishment in Clouds requires collaborative efforts from industry and academia. Abbadi and Alawneh [23], presented a framework for establishing trust in the Cloud. The framework uses the dynamic domain concept. It is composed of the following: Cloud Management Domain (MD), Cloud Collaborating Management Domain (CMD), Organization Outsourced Domain (OD), Organization Collaborating Outsourced Domain (COD), and Organization Home Domain (HD). But, the framework is not enough by itself, and requires further extensions as establishing trust in Clouds is a complex subject. Also, it discusses how the framework could be extended with their previous work on secure virtual infrastructure management. They have considered Clouds resources management and infrastructure properties and differentiated between the secure management of infrastructures data and user's applications data.

Li and Ping [24] analyzed several trust models used in large and distributed environment and then introduced a novel Cloud trust model to solve security issues in cross Clouds environment. Where, customer can choose different providers' services and resources in heterogeneous domains can cooperate. The model is domain based. It divides one CSP's resource nodes into the same domain and sets trust agent. It distinguishes two different roles customer and server. Then, it designs different strategies for them. In this model, trust recommendation is treated as one type of Cloud services just like computation or storage. The model achieves both identity authentication and behavior authentication. The results of emulation experiments show that the proposed model can efficiently and safely construct trust relationship in cross Cloud environment.

19.4 Data Availability

Whenever data is lost, especially valuable data, there is a propensity to scramble to assign blame. Often in the IT world, this can result in lost jobs, lost company revenue, and, in severe cases, business demise. As such, it is critical to understand how much legal responsibility the CSP, per the service level agreement (SLA), has and to ensure that every possible step has been taken to prevent data loss. As with many legal documents, SLAs are often written to the benefit of the provider, not to the customer. Many CSPs offer varying tiers of protection, but as with any storage provider they do not assume liability for the integrity of your data. Creating a trusted SLA for the Cloud that contains explicit statements if data is lost or corrupted is common practice is still under research.

The first work that identified the Cloud middleware services and their interdependencies focusing on application layer is presented in [20] and at Cloud virtual layer is presented in [25]. The work presented by Abbadi [25], is concerned

about defining, exploring, and analyzing middleware self managed services at Cloud virtual layer. Most importantly it discusses the interdependency across such services in context of Cloud environment. It presents a conceptual model of self managed services and identifies the factors, which affect services' decisions. This model helps in understanding the required functions and their interdependency when providing self managed services in Cloud. Also, it helps in realizing the challenges involved in providing automated management functions. Finally, it discusses the challenges and requirements for managing and providing automated services security and privacy by design. It is considered as the first work to explore this area and especially discussing self managed services' interdependency.

The work presented by Abbadi [20], considered as the first work to identify Cloud middleware types focusing on application layer management services and their interdependencies. Where, establishing trustworthy Cloud infrastructure is the key factor to move critical resources into the Cloud. In order to move in this direction for such a complex infrastructure, we virtually split Cloud infrastructure into layers, each layer relies on the services and resources provided by the layer directly underneath it, and each layer services' rely on messages communicated with both the layer directly underneath it and above it. Each two adjacent layers have a specific middleware that provides self-managed services. These services' implementations are based on the layer they serve. Also, different types of middleware services coordinate amongst themselves and exchange critical messages. Then, it demonstrates services interdependencies and interactions using multitier application architecture in Cloud context. Then, it discusses the advantages of middleware services for establishing trust in the Cloud.

The work of Bajpai et al. [26] proposed an authentication and authorization interface to access a Cloud service. The proposed model explains the messages involved in the process of authenticating employees of an enterprise and providing them access of the distributed Cloud services. The trust is established between the end user and the service provider through the authentication and authorization interface. Access control rights of a user for a particular service are considered before granting the service access to the user of that service. Also, to make the system more securely intact, the access rights are not shared with the authentication and authorization interface. Service selection is acquired via monitoring security measures provided by a service provider through Security Service Level Agreements (Sec-SLAs). Security measures are considered while referring the service to an end user in order to provide an end user with a more efficient Cloud service. Denial of service attack, man in the middle attack and robustness of the system are efficiently handled by this methodology that overcomes the drawbacks of previously defined models. In the initial authentication step the enterprise handles the security measures provided by CSP. So, it relieves the end user from up to 80 % of the basics of CSPs in subsequent phases as compared to the models proposed in the past that consider the handling of security measures through end users.

While, Ko et al. [27] establish the urgent need for research in accountability in the Cloud, and outline the risks of not achieving it. By, proposing new approaches in order to increase data accountability. Two trusting approaches have been introduced;

detective and preventive. Detective approach used to identify the occurrence of a privacy or security risk that goes against the privacy or security policies and procedures. While, preventive used to mitigate the occurrence of an action from continuing or taking place at all. Detective approaches complement preventive approaches as they enable the investigation not only of external risks, but also risks from within the CSP. Detective approaches can also, be applied in a less invasive manner than preventive approaches. Also, it presents the trust Cloud framework, which addresses accountability in Cloud via technical and policy based approaches. Where, it can be used to give Cloud users a single point of view for accountability of the CSP.

Campbell et al. [28] proposed the properties and building blocks of a middleware that assured Cloud can support critical missions, where the middleware must include sophisticated monitoring, assessment of policies, and response to manage the configuration and management of trusted resources. Specifically, it considers applications in which assigned tasks or duties are performed in accordance with an intended purpose or plan in order to accomplish an assured mission. Mission critical Cloud may possibly involve hybrid (public, private, heterogeneous) Clouds and require the realization of end to end and cross layered security, dependability, and timeliness. It proposed the properties and building blocks of a middleware to support critical missions. In this approach, it assumed that mission critical Cloud must be designed with assurance in mind. In particular, the middleware in such systems must include sophisticated monitoring, assessment of policies, and response to manage the configuration and management of dynamic systems of systems with both trusted and partially trusted resources (data, sensors, networks, computers, etc.) and services sourced from multiple organizations.

19.5 Data Confidentiality

Another security risk that may occur with a CSP is data confidentiality. It is one of the main concerns for users of public Cloud services. The work proposed by Arasu et al. [29] discusses the main problem of protecting sensitive key data from being accessed by Cloud administrators who have root privileges and can remotely inspect the memory and disk contents of the Cloud servers. While encryption is the basic mechanism that can leverage to provide data confidentiality, providing an efficient database as a service that can run on encrypted data raises several interesting challenges. It outlines the functionality of Cipher base. It has a novel architecture that tightly integrates custom designed trusted hardware for performing operations on encrypted data securely such that an administrator cannot get access to any plaintext corresponding to sensitive data.

The work proposed by Yonghong [30], provides secure database service, but it needs to integrate many security techniques, such as data access control, network transformation control, database queries and privacy protection. It focuses on privacy protection in distributed secure database service architecture, and proposes a new security model which can use the set of attributes consisting of a quasi

identifier to partition data to different database system to achieve privacy protection. The theoretical analysis and experimental results show that the new method is feasible and provide privacy protection and query execution efficiently, and supports horizontal fragmentation and semantic attribute decomposition. Moreover, it proposes an automatic attribute detection partition method and a new security model which partitions data in unencrypted form to distributed secure database servers.

The work proposed by Itani et al. [31] proposed a PasS (Privacy as a Service); a set of security protocols for ensuring the privacy and legal compliance of customer data in Cloud architectures. The security solution relies on secure cryptographic coprocessors for providing a trusted and isolated execution environment in the computing Cloud. It discussed the PasS protocols and described the privacy enforcement mechanisms supported by them. Also, it presented a description of a proof of concept implementation of the privacy protocols. It allows for the secure storage and processing of users; confidential data by leveraging the tamper proof capabilities of cryptographic coprocessors.

Ranchal et al. [32], illustrates an approach for Identity Management with the ability to use identity data on untrusted hosts. The approach is based on the use of predicates over encrypted data and multiparty computing for negotiating a use of a Cloud service. It uses active bundle which is a middleware agent that includes PII data, privacy policies, and a virtual machine that enforces the policies, and has a set of protection mechanisms to protect it. An active bundle interacts on behalf of a user to authenticate to Cloud services using user's privacy policies.

The usage of a Trusted Platform Management (TPM) is to establish trust in the Cloud and provide remote attestation is proposed in [33, 34]. Wang et al. [34] approach combines the public key based homomorphic authenticator with random masking to achieve the privacy preserving for a public Cloud data auditing system. It happened by proposing a privacy preserving public auditing system for data storage security in Cloud environment. It utilize the homomorphic authenticator and random masking to guarantee that Trusted Privacy Auditing (TPA) would not learn any knowledge about the data content stored on the Cloud server during the efficient auditing process, which not only eliminates the burden of Cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files. To support efficient handling of multiple auditing tasks, it explores the technique of bilinear aggregate signature to extend main result into a multi user setting, where, can perform multiple auditing tasks simultaneously. Trusted Cloud proposals generally assert that the Trusted Computing Base (TCB) of the Cloud should be clearly defined and attested to. Extensive analysis shows that the proposed schemes are provably secure and highly efficient.

However, specific characteristics of trust in the Cloud make such solutions difficult to implement in an effective and practical way. The work by Ruan and Martin [33] establishes trust between Cloud entities based on their dynamic behavior which is not accurate and might affect the availability of CSP and their resilience. It presents RepCloud, a reputation system for managing decentralized attestation metrics in the

Cloud. Moreover, it finds that as trust evidence generated by the Trusted Computing Group (TCG) framework can be efficiently transmitted within the Cloud. In a web of nodes with high connectivity and mutual attestation frequency, corrupted nodes can be identified effectively. By modeling this web with RepCloud, it achieved a fine grained Cloud TCB attestation scheme with high confidence for trust. Cloud users can determine the security properties of the exact nodes that may affect the genuine functionalities of their applications, without obtaining much internal information of the Cloud. Also, it showed that as achieving fine grained attestation RepCloud still incurred lower trust management overhead than existing trusted Cloud proposals. Aradhana and Chana [35] determine process for managing trust with specifying trust policies for different Cloud scenarios. Where, trust policies arerepresented in the form of a decision table that helps in the implementation of these policies.

Sato et al. [36] work proposed a trust model to secure Cloud. It proposed a new Cloud trust model. In addition to conventional trust models, it considers both internal trust, and contracted trust that controls CSP. It calls the Cloud platform that meets the Cloud trust model as Security Aware Cloud. In a security aware Cloud, internal trust must be established as the firm base of trust. By implementing TPM of security such as Id management and key management on internal trust, we obtain a firm trust model. Moreover, by controlling levels of quality of service and security by contract, one can optimize Return on Investment (ROI) on service and security delegated to a Cloud.

19.6 Security and Trust Cloud Data Service

In this section, a security and trust service alternative for public Cloud environment is presented in more details. This alternative, EWRDN, can easily and mostly meet all of the previously mentioned security issues in public Cloud environment. Most of Cloud security techniques aim mainly at protecting the data from being altered or viewed. Due to, the nature of the Cloud, where users have no authority over their private data; there are no guarantees to prove integrity of data. That is one reason why organizations do not trust the data services over their private and sensitive data. So, an important question arises about the way to protect data from being showing.

Therefore, how to saves data from attackers with the ability to prove which one has exposed data is a very important point. Also, an agreement about the techniques used to deal with data in case of errors or crashes happened.

19.6.1 EWRDN Service Model

A Novel Watermarking Approach for Data Integrity and Non Repudiation in Rational Databases (WRDN) is introduced [37]. It prevents the impacts of tampering dataset and localizing any changes made. By giving the database owner more control over his

Table 19.1 Difference between WRDN and EWRDN model

	WRDN	EWRDN
Granularity level	Tuple level	Tuple and attribute level
Is a part of	A relational database management system or a database engine	A service and be involved in a trusted authority service coordination
Verifiability	Blind, private	Blind, private, deterministic
Intent	Ownership prove, Data integrity	Ownership prove, data integrity, Tamper detection
Backup	Does not allow	Allow
Trace users activity	Trace some activity (add or modify)	Data owner has the ability to trace all users activity
Eliminated attacks	Insertion and deletion	Insertion, deletion, and alternation
Overhead space	Depends on function used	Depends on the required data quality level and the compression used

data. Besides, it concentrates on proving the data integrity and copyright protection of database against any type of attack. The main idea is to apply WRDN as a trusted security service on cloud computing. But some problems arise. These problems can be summarized in hiding and locking technique. Moreover, one needs to have the ability to recover data if unauthorized changes or errors appeared.

WRDN proves the data ownership and integrity of database. It survives against two types of attacks that face the database (Insertion, Deletion). It is based on adding a watermark over a hidden column then locks this column. It is designed to be a part of Database Management System (DBMS). So, there are no fears over watermark data detection. The main idea of this chapter is creating a data security service over the Cloud. Unfortunately, applying WRDN directly to be a Cloud service is not feasible due to the following reasons: Over the Cloud, there are no guarantees that a CSP will apply the hidden mechanism over the watermark tuple. At the same time, data and the users could be not in the same country.

Therefore, CSP will also have the authority and the ability to unlock and view the watermark column. Moreover, the system will fail enormously to prove changed attributes or to recover data to its origin. To overcome these problems, some enhancement of WRDN model was made. An Enhancement model for WRDN (EWRDN) is presented [10]. It does not prevent copying, but it deters illegal copying by providing a means of establishing the ownership of a redistributed copy. Table 19.1 summarizes the difference between WRDN and EWRDN.

Therefore, the framework is composed to provide security to the data throughout the entire process of Cloud service coordination at a Trusted Third Party (TTP). Figure 19.4 illustrates EWRDN service architecture. First users need to send tuples to EWRDN service. It works as follows:

1. EWRDN service calculates watermark value for each tuple then sends result to next step.

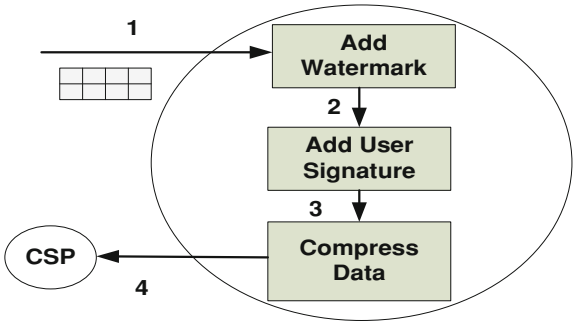

Fig. 19.4 EWRDN service architecture

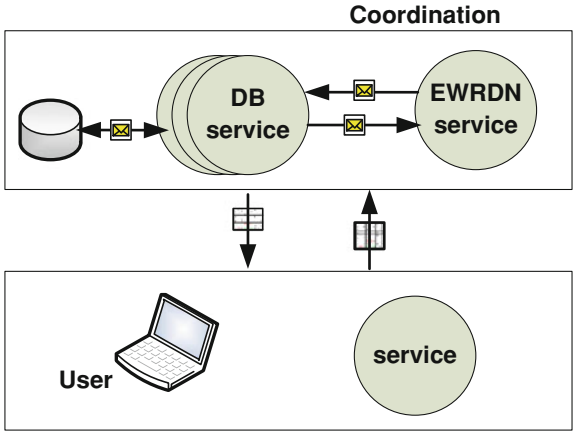

Fig. 19.5 EWRDN service coordination

2. EWRDN service as part of TA service checks over user authority. It adds users Signature using private key (PrK) over each attribute.
3. It compresses signed data, and then saves a copy into operational registry data into service.
4. Send original tuples with watermark value to CSP.

EWRDN service requires the transmission of multiple messages. The challenge lies in coordinating these messages in sequence where the actions performed by the message are executed properly with configuration of overall task. These messages are called Message exchange path (MEP). MEP represents a set of models that provide a group of sequences for the exchange of messages. The more complex an activity, the more context information it will bring. Every activity introduces a level of context into an application runtime environment. Something executing has meaning during its lifetime, and the description can be classified as context. So, a framework is required to provide a means for context information in complex activities to be managed, updated, and distributed to activity participants. Coordination which establishes such a framework is shown in Fig. 19.5.

19.6.2 EWRDN Utilization of Resources

EWRDN does not prevent copying, but it deters illegal copying by providing a means of establishing the ownership of a redistributed copy that can form a trust mean. EWRDN service prevents the worse impacts of tampering data set by localizing any changes made. Besides, it has the ability to recover data to its origin if any changes appear which gives the database owner more control over his data. It uses the compression technique to save tuples and recover them if needed. The data is prevented from any type of attacks by tracing users work to recognize authorization from unauthorized users.

To determine how the compressed data fit, and the estimated disk unit capacity, one needs to apply the following equation

$$\text{Capacity} = \text{Logical\_Data} + (2 \times \text{Free\_Space}) \tag{19.1}$$

The previous equation needs to be calculated for the users when using EWRDN service over the Cloud. That is because more space in the Cloud means extra money. Meanwhile, the previous equation covers space calculation needed to move data over to the Cloud. This proves that in order to; calculate original disk capacity one needs to learn about space of both actual data size and free space on disk. The test experiments made on EWRDN service prove that it consumed less space than WRDN. Where, it has nearly a fixed value of overhead space in EWRDN.

Space complexity depends on compressed values and compression ratio. It has a complexity of $O(1 + \beta)$x n where β is the compressed value between [0,1] and n is the number of attribute. But, β differ according to the importance of data.

$$\text{Space Saving} = 1 - \frac{\text{Compressed Size}}{\text{Uncompressed Size}} \tag{19.2}$$

It has been proven that the type of compression used affect the quality of data. There are two types of compression techniques: Lossless Compression and Loose Compression. Lossless compression technique saves more space than loose compression techniques. Equation 19.2 proves the previous assumptions. It will be found that lossless compression techniques save space of 50 % of the original data size. Loose compression techniques increased the saved space to 60 % of the original data size.

EWRDN service proves data integrity by calculating watermarking data. It adds a watermark with original tuples. Then, it sends original tuples with watermark data to CSP. Also, it saves a copy of watermark value inside operational registry. Where, it gives data owner the ability to prove integrity and ownership of data anytime. Furthermore, it is built to be part of the TTP service coordination. Service Level Agreement (SLA) is made between users and CSP in order to, save data from being missing. Moreover, it adds a user's signature over each attribute being sent to Cloud. It proves data confidentiality and gives data owner the ability to differentiate authorized from

unauthorized users. The main goal behind building EWRDN service is establishing trust in tracing the authorized and unauthorized changes in data services. Data privacy is considered as one of the biggest concerns affecting data storage over the Cloud. Cloud service providers need to find ways to prove and have tools that enable clients to trust their data exchange and storage. Moreover, the service providers need to differentiate between the quality levels provided to the different data owners and users. A data owner needs to track the data at all times with the ability to define errors and data failures, if any, and recover data to its origin. Also, owners need to check over any malicious modification and minimize the effects of server attacks or failures. Moreover, they need to have the same level of assertion every time they operate on the data. At the same time, concurrent users need to log on over the data each time with minimum overhead.

19.7 Conclusion

Clearly, as the use of Cloud environment has rapidly increased, security is still considered the major issue in the Cloud environment. Where, Cloud has become the future technology. Keeping this view in mind, this chapter has attempted to discuss the issues connected with data security. One of the most important issues related to trust and security challenges in Cloud environments is data integrity. Data may suffer from damage during transition operations from or to the CSP. Data owners are wondering about attacks on the integrity and the availability of their data in the Cloud from malicious insiders and outsiders, and from any collateral damage of Cloud services.

It is critical to understand how much legal responsibility the CSPs has and to ensure that all securing procedures have been applied to prevent data deformation, quality and other security threats. Moreover, this can be contacted between clients and CPS in means of a Service Level Agreement (SLA). Creating a trusted SLA for the Cloud that contains clear statements in cases of data loss is a common practice that has an increasing interest of research. A user's privacy and confidentiality risks differ with regards to the terms of service and privacy policy established by the CSP. The location of information in the Cloud effects the data confidentiality protection. The loss of service availability has caused many problems for many customers. Furthermore, data intrusion leads to many problems for the users of the Cloud.

The purpose of this work is to survey the recent research to address the security risks and solutions.

Most of Cloud security techniques aim mainly at protecting the data from being altered or viewed. Users have no authority over their private data; there are no guarantees to prove integrity of data. That is one reason why organizations do not trust the data services over their private and sensitive data. So, an important question arises about the way to protect data from showing. Therefore, how to save data from attackers with the ability to prove which one has exposed data is a very important point.

Also, an agreement about the techniques used to deal with data in case of errors or crashes.

EWRDN service is presented as one of the effective approaches that can handle easily the mentioned trust and security threats in public Cloud environment. It is based on some enhancement made on WRDN technique. It guarantees data integrity, privacy, and non repudiation with the ability to recover data to its origin. The main goal behind building EWRDN service is establishing trust in tracing the authorized and unauthorized changes in data services. It is built to prove data integrity by calculating watermark values. It provides monitoring capabilities between clients and Cloud Service Provider (CSP). Also, it gives users more control over their data by, tracing authorized users activity over database. It proves data confidentiality by adding a user's signature over each attribute. It gives data owner the ability to differentiate authorized from unauthorized users.

References

1. Grandison, T., Maximilien, E.M., Thorpe, S.S.E., Alba, A.: Towards a formal definition of a computing Cloud. In: 6th WorldCongress on Services, SERVICES, pp. 191–192. IEEE Computer Society (2010)
2. Mell, P., Grance, T.: The NIST definition of Cloud Computing. National Institute of Standards, USA (2011)
3. Fensel, D., Facca, F.M., Simperl, E., Toma, I.: Service science. In: Semantic Web Services, chapter 3, pp. 25–35. Springer (2011)
4. Papazoglou, M.P.: Service-oriented computing: concepts, characteristicsand directions. In: Fourth International Conference on Web InformationSystems Engineering, WISE 2003, pp. 3–12. IEEE Computer Society (2003)
5. Carroll, M., Kotzfie, P., van der Merwe, A.: Secure Cloud computing: benefits, risks and controls. In: Information Security SouthAfrica, ISSA, pp. 1–9. IEEE Computer Society (2011)
6. Modi, C., Patel, D., Borisaniya, B., Patel, A., Rajarajan, M.: A survey on security issues and solutions at differentlayers of Cloud computing. J. Supercomput. **63**(2), 561–592 (2013)
7. Zissis, D., Lekkas, D.: Addressing Cloud computing security issues. Future Gener. Comput. Syst. **28**, 583–592 (2012)
8. Modi, C., Patel, D., Borisaniya, B., Patel, A., Rajarajan, M.: A survey on security issues and solutions at differentlayers of Cloud computing. J. Supercomput. **63**(2), 561–592 (2013)
9. Rong, C., Nguyen, S.T., Jaatun, M.G.: Beyond lightning: a survey on security challenges in Cloud computing. Comput. Electr. Eng. **39**(1), 47–54 (2013)
10. El-Zawawi, N., Hamdy, M., El-Gohary, R., Tolba, M.F.: A database watermarking service with a trusted authority architecture for Cloud environment. Int. J. Comput. Appl. **69**(13), 1–9 (2013)
11. Ryan, M.D.: Cloud computing security: the scientific challenge, and a survey of solutions. J. Syst. Softw. **86**(9), 2263–2268 (2013)
12. Pearson, S., Yee, G.: Privacy and Security for Cloud Computing. Springer, London (2013)
13. Elmasri, R.: Fundamental of database systems, 6th edn. (chapter 24). Pearson Education, London (2011)
14. Imran, S., Hyder, I.: Security issues in databases. In: International Conference on Future Information Technology and ManagementEngineering. IEEE Computer Society (2009)
15. DhineshBabu, L.D., Venkata Krishna, P., Mohammed Zayan, A., Panda, V.: An analysis of security related issues in Cloud computing. In: 4th International Conference Contemporary Computing, IC3. Springer (2011)

16. Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L.: On technical security issues in cloud computing. In: IEEE International Conference on Cloud Computing. IEEE Computer Society (2009)
17. Rawat, S., Chowdhary, R., Dr. Bansal, A.: Data integrity of cloud data storages (cdss) in cloud. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **3**(3), 588–592 (2013)
18. Motghare, S., Mohod, P.S., Khandait, S.P., Jaiswal, A.: Framework of data integrity for cross cloud environment using cpdp scheme. Int. J. Adv. Res. Comput. Sci. **4**(4), 55–59 (2013)
19. Abbadi, I.M., Deng, M., Nalin, M., Martin, A., Petkovic, M., Baroni, I., Sanna, A.: Trustworthy middleware services in the Cloud. In: Third International Workshop on Cloud Data Management, CloudDB '11, pp. 33–40. ACM Digital Library (2011)
20. Abbadi, I.M.: Middleware services at Cloud application layer. In: First International Conference Advances in Computing and Communications (ACC 2011), vol. 193 of CCIS, pp. 557–571 (2011)
21. Petkovic, M., Baroni, I., Deng, M., Nalin, M., Marco, A.: Towards trustworthy health platform Cloud. In: SecureData Management, vol. 7482 of SDM, pp. 162–175. Springer (2012)
22. Corradi, A.: Database security management for healthcare SAAS in theamazon awsCloud. In: IEEE Symposium on Computers and Communications, ISCC '12, pp. 812–819. IEEE Computer Society (2012)
23. Abbadi, I.M., Alawneh, M.: A framework for establishingtrust in the Cloud. Comput. Electr. Eng. **38**(5), 1073–1087 (2012)
24. Li, W., Ping, L.: Trust model to enhance security and interoperability of Cloud environment. In: First International Conference, CloudCom, vol. 5931, pp. 69–79. Springer (2009)
25. Abbadi, I.M.: Middleware services at Cloud virtual layer. In: 11th IEEE International Conference on Computer and Information Technology, CIT, pp. 115–120. IEEE Computer Society (2011)
26. Bajpai, D., Vardhan, M., Kushwaha, D.S.: Authentication and authorization interface using security service level agreements for accessing Cloud services. In: 5th International Conference onContemporary Computing-IC3, volume 306 of Communications in Computer and Information Science, pp. 370–382. Springer (2012)
27. Ko, R.K.L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., Lee, B.S.: TrustCloud: a framework for accountability and trust in Cloud computing. In: IEEE World Congress on Services (SERVICES). IEEE Computer Society (2011)
28. Campbell, R.H. Montanari, M., Farivar, R.: A middleware for assured Clouds. J. Internet Serv. Appl. **3**, 87–94 (2012)
29. Arasu, A., Blanas, S., Eguro, K., Joglekar, M., Kaushik, R., Kossmann, D., Ramamurthy, R., Upadhyaya, P., Venkatesan, R.: Secure database as a service with cipherbase. In: ACM SIGMOD International Conference on Management of Data, SIGMOD '13, pp. 1033–1036. ACM Digital Library (2013)
30. Yonghong, Y.: Privacy protection in secure database service. In: International Conference on Networks Security, Wireless Communications and Trusted Computing. IEEE Computer Society (2010)
31. Itani, W., Kayssi, A., Chehab, A.: Privacy as a service: privacy-aware data storage and processing in Cloud computing architectures. In: IEEE International Conference on Dependable, Autonomic andSecure Computing (2009)
32. Ranchal, R., Bhargava, B., Othmane, L.B., Lilien, L., Kim, A., Kang, M., Linderman, M.: Protection of identity information in Cloud computing without trusted third party. In: IEEE Symposiumon Reliable Distributed Systems, SRDS, pp. 368–372 (2010)
33. Ruan, A., Martin, A.: RepCloud: achieving fine-grained Cloud TCB attestation with reputation systems. In: The sixth ACM Workshop onScalable Trusted Computing, STC '11, pp. 3–14. ACM Digital Library (2011)
34. Wang, C., Wang, Q., Ren, K., Lou, W.: Privacy-preservingpublic auditing for data storage security in Cloud computing. In: IEEEINFOCOM, pp. 1–9 (2010)
35. Aradhana, M., Chana, I.: Developing trust policies for Cloud scenarios. In: 2nd International Conference on Computer and Communication Technology, ICCCT, pp. 389–393. IEEE Computer Society (2011)

36. Sato, H., Kanai, A., Tanimoto, S.: A Cloud trust model in a security aware Cloud. In: 10th IEEE/IPSJ International Symposium on Applications andthe Internet (SAINT), pp. 121–124 (2010)
37. Zawawi, N., El-Gohary, R., Hamdy, M., Tolba, M.F.: A novel watermarking approach for data integrity and non-repudiation in rational databases. In: Advanced Machine Learning Technologies and Applications, vol. 322 of Communications in Computerand Information Science, pp 532–542. Springer, Heidelberg (2012)