Secure Data Sharing in the Cloud

Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo

1 Introduction

Cloud systems [1, 2] can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. There is currently a push for IT organisations to increase their data sharing efforts. According to a survey by InformationWeek [3], nearly all organisations shared their data somehow with 74 % sharing their data with customers and 64 % sharing with suppliers. A fourth of the surveyed organisations consider data sharing a top priority. The benefits organisations can gain from data sharing is higher productivity. With multiple users from different organisations contributing to data in the Cloud, the time and cost will be much less compared to having to manually exchange data and hence creating a clutter of redundant and possibly out-of-date documents. With social networking services such as Facebook, the benefits of sharing data are numerous [4] such as the ability to share photos, videos, information and events, creates a sense of enhanced enjoyment in one's life and can enrich the lives of some people as they are amazed at how many people are interested in their life and well-being. For students and group-related projects, there has been a major importance for group collaborative tools [5]. Google Docs provides data sharing capabilities as groups of students or teams working on a project can share documents and can collaborate with each other effectively. This allows higher productivity compared to previous methods of continually sending updated versions of a document to members of the group via email attachments. Also in modern healthcare environments, healthcare providers are willing to store and share electronic medical records via the Cloud and hence remove the geographical dependence between healthcare provider and patient [6]. The sharing of medical data allows

D. Thilakanathan (✉) · R. A. Calvo
Department of Electrical Engineering, The University of Sydney, Sydney, NSW 2006, Australia
e-mail: thilakanathan@hotmail.com

S. Chen · S. Nepal
CSIRO ICT Centre, Cnr Vimiera and Pembroke Rodas, Marsfield, NSW 2122, Australia

S. Nepal and M. Pathan (eds.), *Security, Privacy and Trust in Cloud Systems*,
DOI: 10.1007/978-3-642-38586-5_2,

the remote monitoring and diagnosis of patients without the patient having to leave their house. In one particular scenario, a patient can connect sensors to monitor their ECG to detect any heart problems [7]. They can then run an app on a smartphone device which receives ECG data from the sensors via Bluetooth. The app can then periodically send ECG data to the Cloud. Any authorised doctor or nurse can then get the ECG data via the Cloud without having to visit the patient hence saving costs and time. Therefore, data sharing becomes such a useful feature to implement in Cloud-based environments.

The Cloud however is susceptible to many privacy and security attacks [8, 9]. As highlighted in [10], the biggest obstacle hindering the progress and the wide adoption of the Cloud is the privacy and security issues associated with it. According to a survey carried out by IDC Enterprise Panel [11] in August 2008, Cloud users regarded security as the top challenge with 75 % of surveyed users worried about their critical business and IT systems being vulnerable to attack. Evidently, many privacy and security attacks occur from within the Cloud provider themselves [12] as they usually have direct access to stored data and steal the data to sell to third parties in order to gain profit. There are many examples of this happening in the real world as highlighted in [13]. In today's world, there is a strong need to share information to groups of people around the world. Since the Cloud is riddled with so many privacy issues, many users are still apprehensive about sharing their most critical data with other users.

Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group.

One trivial solution to achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. When the data owner wants to share his data to a group, he sends the key used for data encryption to each member of the group. Any member of the group can then get the encrypted data from the Cloud and decrypt the data using the key and hence does not require the intervention of the data owner. However, the problem with this technique is that it is computationally inefficient and places too much burden on the data owner when considering factors such as user revocation. When the data owner revokes access rights to a member of the group, that member should not be able to gain access to the corresponding data. Since the member still has the data access key, the data owner has to re-encrypt the data with a new key, rendering the revoked member's key useless. When the data is re-encrypted, he must distribute the new key to the remaining users in the group and this is computationally inefficient and places too much burden on the data owner when considering large group sizes

that could be in excess of millions of users. Hence this solution is impractical to be deployed in the real-world for very critical data such as business, government and/or medical related data. In this article, we review existing literature on methods of achieving data sharing in the Cloud that is both secure and efficient.

The rest of this article is organised as follows. Section 2 provides a summary of the existing related literature surveys. Section 3 gives a brief review of some security related definitions and concepts. Section 4 discusses the privacy issues of Cloud computing and what is currently being done to solve those issues. Section 5 provides an in-depth discussion on key management in the Cloud. Section 6 provides a thorough discussion on secure data sharing techniques in the Cloud. Section 7 will review and provide an analysis on the literature. Section 8 concludes the review article.

2 Related Work

This section aims to present a summary of existing review articles related to secure data sharing in the Cloud. The review articles and surveys presented in this section do not focus specifically on secure data sharing in the Cloud, rather the main requirements that will enable it. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. We categorise the existing review articles in two aspects: data sharing and Cloud security.

There have been a number of reviews on security and privacy in the Cloud. Xiao and Xiao [14] identifies the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy and thoroughly reviews the threats to each of the concerns as well as defense strategies. Chen and Zhao [15] outlines the requirements for achieving privacy and security in the Cloud and also briefly outlines the requirements for secure data sharing in the Cloud. Zhou [16] provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud. Wang et al. [17] explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud. Wang [18] carried out a study on the privacy and security compliance of Software-As-A-Service (SaaS) among enterprises through pilot testing privacy/security compliance. They then carry out analysis work on the measurements to check whether SaaS complies with privacy and security standards. The method does not however take into account other Cloud models such as Platform-As-A-Service (PaaS) and in particular Infrastructure-As-A-Service (IaaS), as needed for data sharing. Oza et al. [19] carried out a survey on a number of users to determine the user experience of Cloud computing and found that the main issue of all users was trust and how to choose between different Cloud Service Providers. This is also highlighted in [12] as it states, "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." There

are many examples [13] of insider attacks such as Google Docs containing a flaw that inadvertently shared user documents, MediaMax going out of business in 2008 after losing 45 % of stored client data due to administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on a number of occasions. It's clear from many of the reviews, that the Cloud is very susceptible to privacy and security attacks and currently there is on-going research that aims to prevent and/or reduce the likelihood of such attacks.

The importance of data sharing and the need to ensure privacy and security is discussed in a number of existing articles. Saradhy and Muralidhar [20] review the impact of the Internet on data sharing across many different organisations such as government agencies and businesses. They classify data sharing into data dissemination, query restriction, and record matching. They also provide a framework for secure and useful sharing of data on the internet. Butler [21] describes the issues of data sharing on the Internet where sharing information can allow users to infer details about users. This is useful as it raises awareness to organisations that the data they choose to share with the public can still raise privacy issues and does not guarantee the confidentiality of its users. Mitchley [22] describes the benefits of data sharing from a banking perspective and highlights the privacy issues still affecting it. Feldman et al. [23] discuss the important benefit of data sharing in terms of public health, in particular for education and professional development. Geoghegan [24] discuss a list of organisations that effectively and secure share information via the Cloud. However, it doesn't discuss the methodologies the organisations use to secure data or the downside of these organisations. There is also literature that focus on one aspect of security as well as data sharing; access control. Access control can be used to authorise a subset of users to view confidential data provided they have the right permission. Sahafizadeh and Parsa [25] survey a number of different access control models and evaluates its effectiveness. The survey however, is limited to only software systems and does not take into consideration Cloud systems.

Table 1 shows a summary of the related work. The table categorises the related work in two aspects; Cloud security and Data sharing. The table depicts whether the related work addresses the threats, defense strategies and requirements related to the Cloud or data sharing. The table also depicts whether the related work addresses the impact of the Cloud and/or data sharing in real-world scenarios.

The aim of this paper is to present a comprehensive review of private and secure data sharing in Cloud computing.

3 Privacy Issues in the Cloud

3.1 Privacy Issues

Privacy has many definitions in literature. Some examples of the different definitions of privacy are "being left alone", "the control we have over information about

Table 1 Summary of related work

	Cloud security	Data sharing	Threats	Defense strategies	Requirements	Impact on society
Xiao an Xiao [14]	Y	N	Y	Y	N	Y
Chen and Zhao [15]	Y	Y	Y	N	Y	Y
Zhou [16]	Y	N	Y	Y	Y	Y
Wang et al. [17]	Y	N	N	Y	Y	Y
Wang [18]	Y	N	N	Y	Y	N
Oza et al. [19]	Y	N	Y	N	Y	Y
Saradhy and Muralidhar [20]	N	Y	Y	Y	Y	Y
Butler [21]	N	Y	Y	N	Y	Y
Mitchley [22]	N	Y	Y	N	N	Y
Feldman et al. [23]	N	Y	N	N	N	Y
Geoghegan [24]	N	Y	N	N	N	Y
Sahafizadeh and Parsa [25]	N	Y	N	N	Y	Y

Y yes, *N* no

ourselves" and also "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [26] to name a few. The Organization for Economic Cooperation and Development (OECD) [15] defines it as "any information relating to an identified or identifiable individual (data subject)". The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard [15] is "The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information." From these definitions it is clear that a person has some level of control of what they want to disclose about themselves and want to keep the rest of their information kept secret. Privacy should not be assumed to have the same meaning as confidentiality. Confidentiality is allowing only authorised user's to gain access to that information and no-one else. We briefly explain the need of privacy and confidentiality in a number of fields.

Privacy and Confidentiality of data in Healthcare: In the context of healthcare, patients reveal their health-related information to healthcare professionals in order to diagnose and treat illnesses [27]. The Health Insurance Portability and Accountability Act (HIPAA) [28] provides federal protection of an individual's personal health information and gives individual's rights to their information. The HIPAA Privacy Rule provides protection of patient's personal health information and how external entities such as doctors and nurses can gain access to the patient's data with the patient's consent. As [27] argues, since the patient decides to share their data with one or more healthcare professionals, their data is no longer private, but confidential.

Privacy and Confidentiality of data in Social Networking: Social networking has changed the lives of today's generation. There are many social networking sites with millions of users communicating with each other. Some examples are Facebook, Twitter, MySpace, Blogger, Flickr, digg, YouTube and the list goes on. Internet

privacy has been determined as the "right to be left alone" [29]. The technology that is built to support social networking does not effectively support privacy and may even sell personal information about the individual to third parties and it is mainly up to the individual to disclose information while maintaining privacy. The individual needs to make sure that they do not unknowingly disclose personal information about themselves. Simply disclosing their age, suburb and nationality is enough for malicious users to identify the person. Facebook had undergone scrutiny in the past for not strengthening its privacy measures on user profiles as private photos could still be viewed by non-private viewers through a friend-of-a-friend by simply having a friend comment on it [30].

Privacy and Confidentiality of data in Government: Nearly all governments collect information about its citizens and residents such as education, finance, gender, loans, earnings, medical costs, criminal offences and so on [31]. Governments also release data to the open public for its citizens to view. This may not guarantee the privacy of its citizens as some user may be able to infer information about a particular user through government data. In the United States for example, the Privacy Act of 1974 aims to protect an individual's privacy [32]. According to the Act, individuals have the right to see information the government has about them, modify or remove incorrect information, and also sue the government for violations of the Act including but not limited to, unauthorized access of personal information. Governments need to keep data private from other governments too [33] as the results can be devastating if information is leaked such as the WikiLeaks controversy [34].

Privacy and Confidentiality of data in Education: Schools usually collect all students personal and health information. These include name, phone, address, contact details, finance details, medical history and family history to name a few. It is usually strongly implied that schools keep this information confidential and private [35]. Failure to keep student personal information confidential can result in safety consequences for the student.

Privacy and Confidentiality of data in Corporations: Major businesses and organisations also require privacy and confidentiality of their data. Leakage of sensitive information can result in revenue loss for a company even to the point of shutting down.

3.2 Types of Attacks on the Cloud

There are a number of types of privacy and security attacks in the Cloud. The following contains a summary of the common types of attacks that may occur in the Cloud.

- *XML Signature Wrapping Attacks*—Using different kinds of XML signature wrapping attacks, one can completely take over the administrative rights of the Cloud user and create, delete, modify images as well as create instances [36].

- *Cross site scripting attacks*—Attackers can inject a piece of code into web applications to bypass access control mechanisms. Researchers found this possible with Amazon Web Services [36] in November 2011. They were able to gain free access to all customer data, authentication data, tokens as well as plaintext passwords.
- *Flooding Attack Problem* —Provided a malicious user can send requests to the Cloud, he/she can then easily overload the server by creating bogus data requests to the Cloud [37]. The attempt is to increase the workload of the Cloud servers by consuming lots of resources needlessly.
- *Denial-of-Service Attacks*—Malicious code is injected into the browser to open many windows and as a result deny legitimate users access to services.
- *Law Enforcement Requests*—When the FBI or government demand a Cloud Service Provider access to its data, the Cloud Service Provider is least likely to deny them. Hence, an inherent threat to user privacy and confidentiality of data.
- *Data Stealing Problem*—A term used to describe the stealing of a user account and password by any means [37] such as through brute-force attacks or over-the-shoulder techniques. The privacy and confidentiality of user's data will be severely breached. A common mechanism to prevent such attacks is to include an extra value when authenticating. This value can be distributed to the right user by SMS and hence mitigate the likelihood of data confidentiality issues.

3.3 The Motives of a Malicious User

While there is many literature on what can be done to secure a system against attackers, very little discusses the types of attackers and their motivations for carrying out such attacks. In reality, there are many different types of attackers with different reasons to attack users [38, 39]. The following contains some examples.

- *To steal valuable data*—Hackers love to steal data as some data stored in the internet are valued millions of dollars. With access to valuable data, they can then generate revenue, for example, WikiLeaks [34].
- *To cause controversy*—Some attackers purely love the thrill and excitement of causing chaos and the internet, and similarly the Cloud, is one of the best mediums to target mainly because of the popularity of the internet as well as it being more likely to steal data over the internet in comparison to a personal computer system.
- *To get revenge*—Former workers who were recently stripped of their position at an organisation may express their dissatisfaction by hacking the organisation's network. When an organisation makes use of the Cloud, this becomes all too easy for the former employee and there have been many cases of this happening in the real-world. For instance, there was the case of a former employee who managed to get access to the Cloud provider's server and deleted an entire season of a children's TV show [12].
- *To help*—A hacker, in contrast, may also try to help an organisation by identifying the security flaws in their system. A hacker may be confident enough to bypass

the existing security protocol and implant his or her own mechanisms to expose the protocol.
- *To prove intellect and gain prestige*—Attackers may also want to show off their skills and gain prestige among their social skills if they were able to hack a large organisation with solid security mechanisms. Some hackers make a career out of hacking organisations.
- *Are just curious*—Some hackers are curious to learn something about a company and/or organisation. These kinds of hackers don't usually have malicious intent as they may not be aware of breaking security rules however it does not mean these hackers are less dangerous whatsoever.

3.4 Examples of Real World Issues

There are many examples of real world privacy and security issues that have affected the Cloud. These issues have provided a barrier to the worldwide adoption of the Cloud. We present these issues as a list.

- In 2007, Salesforce.com leaked customer contact lists after an employee revealed the list to a phisher, and in turn allowed scammers to target phishing attacks against Salesforce customers [40].
- In April 2011, Sony was involved in a massive security blunder that potentially gave away 100 million credit card numbers. Hackers claimed to have stolen millions of credit card numbers from Sony's PlayStation Network [41].
- Google revealed in June 2011 that hackers from China stole passwords and attempted to break into email accounts to steal information [42]. More than 100 people were affected and included senior government officials. People started to argue whether this, and the Sony incident was start of the downfall of Cloud computing [43].
- Hotmail and Yahoo Mail users were also targetted in phishing attacks [44, 45]. The attacks involved a user either clicking a malicious link in the email or even viewing the email itself which would then run malicious code and attempt to compromise the user's account.
- Google Docs contained a flaw that inadvertently shared user docs with unauthorised users [13]. Other users could access and edit docs without the Google docs owner permission.
- There was also the issue of MegaUpload leaving its millions of legitimate users in cyber-limbo [46]. MegaUpload was a site where people could share files. Unfortunately due to the amount of illegal content such as pirated films and television shows, the site was forced to shut down in early 2012.
- A Distributed Denial-of-Service (DDoS) attack on Amazon Web Services forced many companies to shut down temporarily, such as Bitbucket [47].
- Facebook was the target of phishing attacks in early 2012 which attempted to steal user accounts and learn financial information [48]. Once accounts were stolen, the

user's profile would be locked out and the profile picture would change. In fact, Facebook has been the target of a number of phishing attacks such as Ramnit [49] which affected upto 45,000 users.

Each of these attacks contributes heavily to user suspicion and trust of storing sensitive data in the Cloud. From this list, it is clear why users are apprehensive about storing their most sensitive data in the Cloud and in order to gain trust of using the Cloud to store critical data, mechanisms need to be implemented to guarantee data is kept both confidential and secure from unauthorised users.

3.5 Recommended Guidelines for Private and Secure Cloud

According to [50], the above issues may have the following impacts on the Cloud:

Governance—Organisations usually have standards, practices, protocols, policies and procedures which employees must abide by and this can cover application development, testing, implementation, monitoring and so on. When an organisation makes use of Cloud services, there is always the possibility that employees bypass these rules, as there is a lack of organisational rules regarding the Cloud.

Compliance—Refers to an organisation's responsibility to operate in agreement with established laws, regulations, etc. There are a number of privacy and security laws within different countries, states, and so on and when using the Cloud, one has to consider whether they are likely to breach any privacy or security law as data stored in the Cloud is usually stored in multiple locations around the world, at times without the knowledge of the user.

Trust—It is a well-known fact that when a user or organisation chooses to outsource their data to the Cloud, they relinquish full control of their data and provide a high level of trust to the Cloud provider. As discussed in the introduction as well as in the next section, most data privacy and security attacks come from insider attacks. The Cloud provider usually has direct access to data and hence is more likely to steal data for illegal purposes. In terms of trust, there is also the issue of data ownership such as who owns the data, and contracts specifying whether the Cloud has some or no access to parts of its data.

Architecture—The architecture of the Cloud needs to be designed in a way to prevent privacy and security attacks. For instance, IaaS Cloud providers can provide Virtual Machine Images to consumers. An organisation which makes use of these images, may store very critical data. An attacker may examine the images to see whether they leak information. An attacker may also supply a corrupted virtual machine image to users and hence steal confidential data. It is important that the architecture of the Cloud is developed such that it ensures privacy and security as attackers are always on the lookout for security holes in Cloud architecture.

Identity and Access Management—As data sensitivity and privacy is becoming an ever-increasing issue of organisations, the identity and authorisation framework

present in the organisation may not extend into the Cloud and malicious users may be able to gain unwarranted access to data they are not allowed to.

Software Isolation—With multi-tenant Cloud computing architectures, computations for different consumers are carried out in isolation even if the software remains in a single software stack. Applications running in the Cloud are susceptible to attack and compromise and hence isolation is needed to prevent such attacks.

Data Protection—Data stored in a public cloud usually reside with other data from other organisations. When an organisation places their sensitive data in a public cloud, they must account for the possible privacy and security attacks by ensuring proper access control mechanisms such as encryption. Since data is stored "in the open", this provides a world of opportunities for malicious users to steal data. Similar concerns exist when data is in transit.

Availability—As defined in the NIST Security and Privacy Guidelines [50], availability is the extent to which an organisation's full set of computational resources is accessible and usable. Attacks such as Denial-of-Service attacks, server downtime, natural disasters affect availability and can affect stored data and more importantly causes downtime which affects an organisation greatly.

Incident Response—An incident response is an organised method of dealing with the consequences a security attack. The Cloud containing many layers such as application, operating system, network, database and so on, and a log is generated of any event as part of its intrusion detection system. Such complexity in its layers means it will take many hours to identify an attack in the Cloud.

4 Protection from Privacy and Security Attacks

In this section, we discuss what is currently being done to protect and/or mitigate the privacy and security attacks on the Cloud.

Currently, there is on-going research on how to protect the confidentiality and security of data stored in the Cloud. Cavoukian [51] proposes implementing security as a service in the Cloud using a discretion algorithm and also implementing an intrusion detection system for the Cloud. Sabahi [52] argues the need for a flexible and user-centric identity management such that in the future a user will not have to re-enter credentials for a website and can rely on an identity service to manage website access.

In order to protect a user's data confidentiality, some form of access control needs to be implemented in the Cloud. Access control should allow a user to choose who can view his data and who shouldn't. Access Control Lists (ACLs) were originally used [53], however, it was not effective as it was too coarse-grained and was not scalable; one of the primary features of the Cloud.

An alternative and effective access control technique is encryption. Encrypting data ensures data is protected from unauthorised users. There are two types of encryption; symmetric and asymmetric encryption. In symmetric encryption, a key is used to encrypt the data to make it virtually unreadable. The same key is also used to

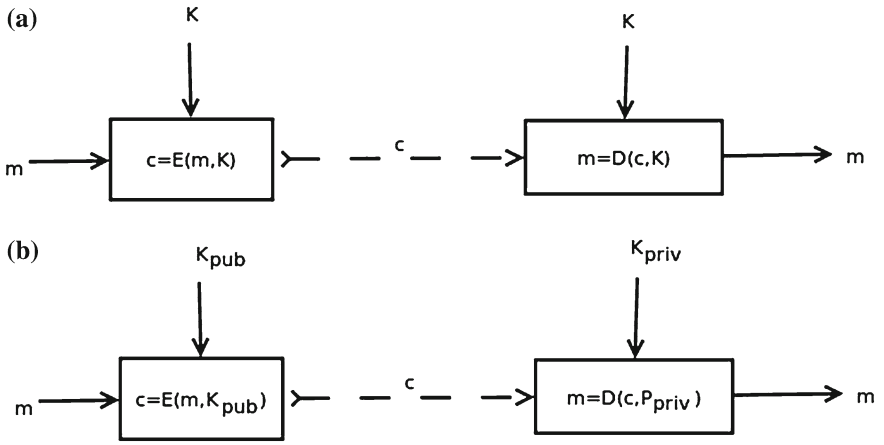

Fig. 1 Asymmetric encryption

convert the unreadable ciphertext to its original plaintext. This key must be kept confidential with the data owner. In asymmetric encryption, a public and private key is used to encrypt and decrypt data. A user encrypts the data using another person's public key. The other person then uses his private key to decrypt the data. The public key can be broadcast to the world but the private key must remain confidential with the user.

When involving data in the Cloud, encryption thus becomes crucial. Many works in literature suggest the need for encrypting data in the Cloud in some form or another. Huang et al. [13] states that encryption must occur in transit, at rest and on backup media. Gentry [54] proposes the use of homomorphic encryption to keep data secure and confidential. With homomorphic encryption, it is possible to perform operations such as querying and searching on encrypted data without ever having to decrypt the data and hence exposing privacy. Yao et al. [55] propose a system called 'TrustStore' which encrypts and partitions data on the client side and sends each partition to different Cloud storage providers. This greatly enhances the confidentiality of data as the chance of compromising two or more storage providers is low. However, it doesn't handle the case of data sharing and collaboration, which is the focus of this paper.

When considering data sharing and collaboration, simple encryption techniques do not suffice, especially when considering key management. To enable secure and confidential data sharing and collaboration in the Cloud, there needs to first be proper key management in the Cloud. This will be explained in detail in a later section.

A few research problems currently exist such as how do we manage and distribute keys for each granted user? How do we revoke their rights from accessing the data? Once a user is revoked rights, is it possible for a user to rejoin the group with the same rights?

We now discuss and review literature based on key management in the Cloud, which will later follow on to data sharing and collaboration.

5 Secure Data Sharing in the Cloud

In this section, we discuss the growing need for data sharing and the benefits of data sharing via the Cloud. We list the requirements of data sharing in the Cloud followed by the traditional approach to sharing data via the Cloud and why this isn't effective. We also discuss the key management problem and review a number of works that address this problem. We then review recent works that aim to provide private and secure data sharing in the Cloud and discuss the latest techniques used to achieve this.

5.1 Why Data Sharing is Important

Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organisations aiming to gain profit. Historically, many people viewed the computer as "impersonal giants" who threatened to cut jobs of many people through automation. However, in recent times, it has been welcomed by a huge number of people as it has become significantly social [56]. It is thus not surprising that more and more people are demanding data sharing capability on their phones, computers and even recently Smart TVs.

People love to share information with one another. Whether it is with friends, family, colleagues or the world, many people benefit greatly through sharing data. Some of the benefits include:

- *Higher productivity*: Businesses get more work done as well as making collaboration with peers much more efficient and hence is key to satisfying their business goals. Hospitals also benefit from data sharing and this has led to the lowering of healthcare costs [57]. Students also benefit when working on group projects, as they are better able to collaborate with members and get work done more efficiently.
- *More enjoyment*: Many people of any age, gender or ethnicity can connect with friends, family and colleagues to share their experiences in life as well as catch up with others via social networking sites such as Facebook or MySpace. Employees and enterprise users can share their experiences through sites like Yammer. People can also share videos on YouTube or photos on Flickr, which can provide greater enjoyment with some people. In the past, connecting to a loved one in a different country was not possible except through letters. Hence social data sharing generally provides people with a rich experience as the sharing of personal information can provide people with deeper and stronger relationships.
- *To voice opinions*: Some people prefer to share information to the world in order to voice an opinion. Many people want to be heard and use social networking sites to

promote their opinion, which was not possible unless they formed protests. People are now using social networking sites such as Facebook, Twitter and YouTube to raise awareness about real issues in the world. Although, some campaigns have led to violent protests, online campaigns usually inform people of issues and encourage people to help a cause.

Data sharing is becoming increasingly prevalent in many industries and organisations. Hospitals are now benefitting from data sharing as this provides better, safer care of patients. There is now no need to repeat medical history every time a new health professional is consulted which means no more unnecessary tests. Hence, the health professional gets a more complete picture of medical history [57]. There is also a strong focus for the sharing of research data [58]. According to Feldman et al. [59], there is growing support for the sharing of research data in order to accelerate the pace of scientific discovery. Such sharing will allow for more rapid translation of science to practice. Financial institutions also benefit from data sharing and benefits include better customer support and better understanding of the needs of the customer [60]. Shared data can be used to improve modeling, analysis and risk tools.

With the advancements in Cloud computing, there is now a growing focus on implementing data sharing capabilities in the Cloud. With the ability to share data via the Cloud, the number of benefits increases multifold. As businesses and organisations are now outsourcing data and operations to the Cloud, they benefit further with the ability to share data between other businesses and organisations. Employees also benefit as they can share work and collaborate with other employees and can also continue working at home or any other place such as the library. They don't need to worry about losing work as it is always in the Cloud. With social users, the ability to share files, including documents, photos and videos with other users provides great benefit to them. The shutdown on the MegaUpload website where people could upload and share files with other people in the Cloud left millions of users around the world devastated [46]. The amount of illegal contents such as pirated films and full television shows forced the website to be shut down. This exemplifies the strong need for data sharing in the Cloud.

However, the main problem with data sharing in the Cloud is the privacy and security issues. As discussed in Sect. 4, the Cloud is open to many privacy and security attacks, which make many users wary of adopting Cloud technology for data sharing purposes. The work done to prevent the privacy and security issues of the Cloud as discussed in Sect. 4.2, is not sufficient enough when considering data sharing aspects. We next discuss the main requirements for secure data sharing in the Cloud and then review literature on securing data sharing in the Cloud.

5.2 Requirements of Data Sharing in the Cloud

To enable data sharing in the Cloud, it is imperative that only authorised users are able to get access to data stored in the Cloud. We summarise the ideal requirements of data sharing in the Cloud below.

- The data owner should be able to specify a group of users that are allowed to view his/her data.
- Any member of the group should gain access to the data anytime without the data owner's intervention.
- No other user, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider.
- The data owner should be able to revoke access to data for any member of the group.
- The data owner should be able to add members to the group.
- No member of the group should be allowed to revoke rights of other members of the group or join new users to the group.
- The data owner should be able to specify who has read/write permissions on the data owner's files.

We now look at the privacy and security requirement of data sharing in the Cloud. Achieving these requirements in the Cloud architecture can go a long way to attracting large numbers of users to adopting and embracing Cloud technology.

- *Data Confidentiality*: Unauthorised users (including the Cloud), should not be able to access data at any given time. Data should remain confidential in transit, at rest and on backup media. Only authorised users should be able to gain access to data.
- *User revocation*: When a user is revoked access rights to data, that user should not be able to gain access to the data at any given time. Ideally, user revocation should not affect other authorised users in the group for efficiency purposes.
- *Scalable and Efficient*: Since the number of Cloud users tends to be extremely large and at times unpredictable as users join and leave, it is imperative that the system maintain efficiency as well as be scalability.
- *Collusion between entities*: When considering data sharing methodologies in the Cloud, it is vital that even when certain entities collude, they should still not be able to access any of the data without the data owner's permission. Earlier works of literature on data sharing did not consider this problem, however collusion between entities can never be written off as an unlikely event.

5.3 Traditional Approach

A trivial solution to data sharing and collaboration in the Cloud involves a data owner distributing encryption keys to every user he authorises. Each user that has authorised access can then get the encrypted data from the Cloud and decrypt the data using the

supplied key. This ensures that no unauthorised user gets access to data even if he manages to download the ciphertext from the Cloud as he does not possess the key for decryption.

This solution however, is not both efficient and effective. Once the data owner decides to revoke a user from accessing their data, one trivial solution would be for the data owner to decrypt the data and re-encrypt the data again, this time with a new key and distribute this new key to the remaining users in the group. This can become extremely costly and places a huge burden on the data owner when considering group sizes in excess of thousands to millions of users. Furthermore, as members of the group continually join and leave, continually re-encrypting data and sending re-encryption keys to a group of this size becomes impractical for the data owner and infeasible to implement in the real world. Currently, there is ongoing research on this problem.

Zhao et al. [61], suggests a progressive elliptic curve encryption scheme (PECE) where a piece of data is encrypted a number of times using multiple keys and later decrypted using one key. Data sharing involves one user, say Alice, encrypting her data using her private key and storing the encrypted data to the Cloud. Another user, say Bob, sends a request for data access permission by sending his public key to Alice. Alice sends a credential to the storage provider for re-encryption of data and sends a credential to Bob to decrypt the data. This is an effective technique as it keeps data confidential as data is encrypted through the entire stages thus never allowing a malicious user to view the plaintext data. This technique also does not allow the permission bearer, in our case Bob, to share the file owned by the permission holder, in our case Alice, with other users. The main problem however with this technique is that it requires the data owner to be online at all times and hence makes it inefficient for everyday users. This technique also assumes the private key of the Cloud provider is shared with the data owner. Realistically, no system administrator would want to share their keys with users and thus making it impractical to be deployed.

5.3.1 The Need for Key Management in the Cloud

Key management is anything you do with a key except encryption and decryption [62] and covers the creation/deletion of keys, activation/deactivation of keys, transportation of keys, storage of keys and so on. Most Cloud service provider's provide basic key encryption schemes for protecting data or may leave it to the user to encrypt their own data.

Either way, there is a need to encrypt data that is involved in the Cloud. But how do we handle the keys that are used for encryption? Where should the keys be stored and who has access to those keys? How do we recover data if keys are lost? Both encryption and key management are very important to help secure applications and data stored in the Cloud [63]. Especially in recent times, there has been a strong need for Cloud providers to adopt a robust key management scheme for their services. However, there are still key management issues affecting Cloud computing as described in [64]. We discuss the 3 requirements of effective key management below.

- *Secure key stores*: The key stores themselves must be protected from malicious users. If a malicious user gains access to the keys, they will then be able to access any encrypted data the key is corresponded to. Hence the key stores themselves must be protected in storage, in transit and on backup media.
- *Access to key stores*: Access to the key stores should be limited to the users that have the rights to access data. Separation of roles should be used to help control access. The entity that uses a given key should not be the entity that stores the key.
- *Key backup and recoverability*: Keys need secure backup and recovery solutions. Loss of keys, although effective for destroying access to data, can be highly devastating to a business and Cloud providers need to ensure that keys aren't lost through backup and recovery mechanisms.

Tim Mather [65] states that key management in enterprises today are broken and that key management in the Cloud is a failed model that is neither effective nor scalable. What cloud computing needs are standards. Fortunately there are a number of standards of key management in the Cloud and is briefly described below.

- *OASIS Key Management Interoperability Protocol (KMIP)*—Used to define a single, comprehensive protocol for communication between encryption systems and enterprise key management systems [66, 67]. KMIP is becoming a widely accepted standard in industry and are looking to implement it within their frameworks.
- *NIST SP 800-57*—Provides general guidelines on key management, the recommended types of encryption schemes and protection requirements as well as information of key recovery [68].
- *IEEE 1619.3 Key Management*—Covers storage encryption and key management mainly for IaaS storage [64]. The standard has been disbanded since December 2010.
- *ISO/IEC 11770-5:2011*—Specifies key establishment mechanisms for multiple entities to provide procedures for handling cryptographic keys used in symmetric and asymmetric encryption algorithms [69].
- Other standards include ISO 11568-2:2012 [70], and IETF KeyProv.

Bruce Schneier [63] quotes "Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system". Pate and Tambay [63] describes that since technology is so broad as it spans various operating systems, storage, encryption and key management, virtualization and VM mobility and Cloud, key management solutions in the Cloud needs to be broader. Luther [62] on the other hand, states that key management is harder than cryptography where cryptography all boils down to math, key management involves technology, people, and processes. He states that strong encryption is nearly impossible to beat compared to key management which is not as robust.

5.3.2 Review of Works on Key Management

Lei et al. [71] illustrated the need for proper key management in the Cloud environment. A Cloud Key Management Infrastructure (CKMI) is proposed which contains

a Cloud Key Management Client (CKMC) and Cloud Key Management Server (CKMS). The protocol includes objects which contain keys and certificates, etc, the operations upon them such as creation, deletion, retrieval and updating of keys, certificates, and also attributes related to the object in question such as the object identifier. The method is effective for proper key management however, if the server is broken, all the user's data is lost and there is no proper backup and recovery mechanism, a key requirement of key management as described above.

Huang et al. [13] worked to build on top of the Leakage Resilient Authenticated Key Exchange (LR-AKE) first proposed by Fathi et al. [72] and proposed the LR-AKE Cluster mode protocol for effective key management. The LR-AKE involves the user remembering a password while additionally storing a high-entropy secret on the client machine to allow communication between different servers. In the LR-AKE Cluster mode, the client generates authentication secrets for each server and partial data keys. Each pair authenticates and communicates with each other to combine partial keys to reveal full data keys when user requests. The main weakness with this protocol is that if any one of the servers or the client fails, the data is lost as the keys used to access the data will not be available. The LR-AKE Cluster+ mode builds on the LR-AKE Cluster mode, where aside from the user personal password, the client chooses a random password (256 bits long) and another device (e.g., a USB drive) stores this random password as well as the authentication secrets for added security and higher availability. Secrets are required from both parties of the communication and hence data still remains information-theoretically secure and confidential. One of the drawbacks to this approach is that it requires the maintenance of a number of servers and the client, which adds unwanted complexity when trying to attract large number of users to the Cloud.

Sanka et al. [73] proposed capability lists for effective key management and data access where the data owner does not have to be online at all times. The model involves using a capability list where the data owner creates a list containing an entry for each user and the permissions for file access and stores this list in the CSP. When a user requests access to a file, he requests access to the file directly to the CSP, hence data owner does not have to be online at all times and only needs to be online when registering new users or revoking users from the list. The model is secure and confidential against the Cloud and unauthorised users since they never know the contents of the encrypted data since the key is a shared symmetric key between the data owner and user. The main issue with the model however, is that it assumes the CSP will not alter the capability list. The CSP has access to the unencrypted capability list and can maliciously alter or shut out files from users.

Bennani et al. [74] proposes a model which replicates the database in the cloud n times where n represents the number of roles. When a role is revoked access rights, the corresponding database is removed. Changing a roles access rights leads in the worst case to the creation from scratch a new view and re-keying the corresponding database. One of the main problems with this model is that it is infeasible to implement since it introduces high redundancy and hence is not efficient.

Table 2 Summary of literature on key management in the Cloud

Method	Data/Key redundancy	Data owner online at all times	Confidentiality preserved from CSP	Single point of failure
Lei et al. [71]	N	N	Y	Y
Huang et al. [13]	Y	N	Y	N
Sanka et al. [73]	N	N	N	N
Bennani et al. [74]	Y	N	Y	N

Y yes, *N* no

5.3.3 Discussion

The Table 2 shows a summary of the existing literature based on key management in the Cloud. The works that were reviewed had a strong focus on preventing the need for the data owner to be online at all times. Many of the works that were reviewed also had a strong focus on preventing the Cloud from viewing any of the plaintext at all times. However, in terms of achieving proper key management in the Cloud, some form of redundancy had to be introduced in some of the works.

Proper key management in the Cloud can lead to more secure and confidential sharing of data in the Cloud. A poor key management system can lead to the complete unreliability of the Cloud and can also lose trust from its consumers. Hence it is imperative that more research needs to done in achieving a more robust key management for the Cloud not only to attract more consumers and build trust but also to provide a foundation for secure and private data sharing in the Cloud.

5.4 Recent Approaches

In this section, we provide a review on current works of literature on enabling secure and confidential data sharing in the Cloud.

5.4.1 Attribute-Based Encryption

Attribute-Based Encryption (ABE) is one effective and promising technique that is used to provide fine-grained access control to data in the Cloud. Initially, access to data in the Cloud was provided through Access Control Lists (ACLs) however, this was not scalable and only provided coarse-grained access to data [53]. Attribute-Based encryption first proposed by Goyal et al. [75] provides a more scalable and fine-grained access control to data in comparison to ACLs.

Attribute-Based Encryption is an access control mechanism where a user or a piece of data has attributes associated with it. An access control policy is defined and

if the attributes satisfy the access control policy the user should be able to get access to the piece of data.

There are two kinds of ABE [53], which are described as follows.

- Key-Policy ABE (KP-ABE): The access control policy is stored with the user's private key and the encrypted data additionally stores a number of attributes associated with the data. A user can only decrypt the data if the attributes of the data satisfy the access control policy in the user's key. The access control policy is usually defined as an access tree with interior nodes representing threshold gates and leaf nodes representing attributes.
- Ciphertext-Policy ABE (CP-ABE): Essentially the converse of KP-ABE. The access control policy is stored with the data and the attributes are stored in the user's key.

ABE for Data Sharing and Collaboration

ABE is also used for data sharing and collaboration works. Tu et al. [76] made use of CP-ABE in the context of enterprise applications and also developed a revocation mechanism that simultaneously allows high adaptability, fine-grained access control and revocation. The department assigns users a set of attributes within their secret key and distributes the secret key to the respective users. Any user that satisfies the access control policy defined by the data collaborator can access the data. When a user is revoked access rights, the data is re-encrypted in the Cloud rendering the revoked user's key useless. The scheme is proven to be semantically secure against chosen ciphertext attacks against the CP-ABE model. However, the scheme is not elegant in the case of user revocation since the updating of ciphertexts after user revocation places heavy computation overhead even if the burden is transferred to the Cloud.

Li et al. [77] leverages ABE in the context of the sharing of personal health records (PHR) in the Cloud. Their framework consists of a public domain consisting of users who make accesses on professional records such as doctors, nurses and medical researchers, and also personal domain, which consist of users who are personally associated with the data owner such as family and close friends. Role attributes are assigned to the users in the public domain that represents their professional role and they retrieve their secret keys from an attribute authority. This is effective as the data owner need not be online at all times. In terms of access control, data owners specify role-based fine-grained access control policies for their PHR files. Using role-based access policies greatly reduces key management overhead for owners and users as the owner does not have to manage keys for each individual user.

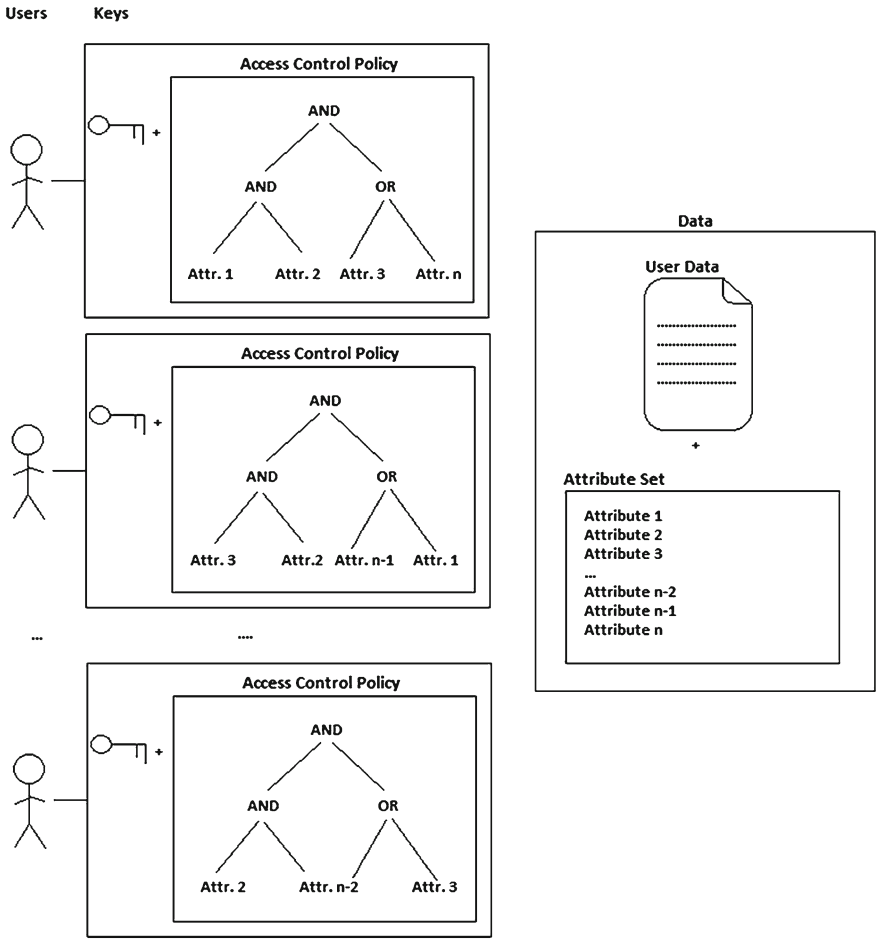

Fig. 2 Key-policy attibute-based encryption

5.4.2 Proxy Re-encryption

Proxy Re-encryption is another technique that is fast becoming adopted for enabling secure and confidential data sharing and collaboration in the Cloud.

Proxy Re-encryption [78] allows a semi-trusted proxy with a re-encryption key to translate a ciphertext under the data owner's public key into another ciphertext that can be decrypted by another user's secret key. At no stage will the proxy be able to access the plaintext. Researchers have utilized proxy re-encryption in relation to the Cloud and in particular for secure and confidential data sharing and collaboration in the Cloud.

We demonstrate a basic Proxy Re-encryption scheme with the diagram below. A user, say Alice, encrypts her data m, using her public key. When she wants to

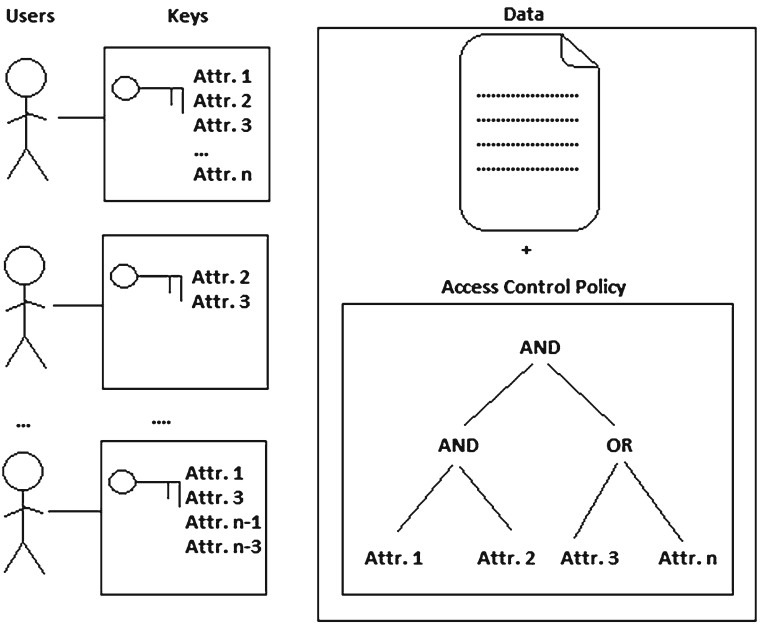

Fig. 3 Ciphertext-policy attribute-based encryption

Fig. 4 A basic proxy re-encryption scheme

share the data with another user, say Bob, she sends the encrypted data to a proxy. The proxy then converts the data encrypted under Alice's public key into data that is encrypted under Bob's public key and sends this to Bob. Bob can now use his private key to decrypt the ciphertext and reveal the contents.

Proxy Re-encryption for Data Sharing and Collaboration

A number of works in literature have propositioned proxy re-encryption for enabling secure and confidential data sharing and collaboration in the Cloud.

Tran et al. [79] uses the idea of Proxy Re-encryption scheme where the data owner's private key is divided into two parts. One half is stored in the data owner's machine while the other is stored in the Cloud proxy. The data owner encrypts the data with half his private key, which then gets encrypted again by the proxy using his other half of the key. Another user who has been granted access rights will then have the same key divided with different parts. One half will be kept on the granted user's machine and the other half stored on the Cloud proxy. The user who has access

rights can then retrieve the data as the proxy will decrypt the ciphertext with half the user's private key in the proxy and then decrypt again on the user's side to retrieve the full plaintext. When the data owner wishes to revoke a user from accessing the data, he simply informs the Cloud proxy to remove the user's key piece. The main strength with this scheme is that it doesn't require re-encryption if a user's rights are revoked and hence saves on computation costs, especially when considering the large number of users in groups. As with the PECE scheme described above [61], this scheme doesn't allow outsiders to view the original plaintext at any point as the data remains in an unreadable format in the Cloud. Only users with granted access rights can view the original plaintext. However, the main problem with this scheme is that of collusion attacks; if a revoked user and the proxy collude, that user then has access to the other entire users private key in the group. Also, the proxy may suffer from too many encryption and decryption operations. The model also assumes that the data owner has already given permission to a number of users to access the data.

5.4.3 Hybrid ABE and PRE

ABE and Proxy Re-encryption have also been used in combination with each other to provide extra security and privacy for data sharing and collaboration in the Cloud. A number of works in literature are taking advantage of combining the power of the two schemes to provide a more robust and guarantee further trust in the data owner for the secure sharing of data in the Cloud.

Yu et al. [80] was one of the first works, which combined ABE, Proxy Re-encryption and lazy encryption schemes for Cloud privacy and security. The scheme works by data owner encrypting his data using a symmetric key and then encrypting the symmetric key using a set of attributes according to KP-ABE scheme. A new user joins the system when the data owner assigns an access structure and its corresponding secret key and distributes this to the new user. To revoke a user, the data owner determines the minimum number of attributes, which will never satisfy the revoked user's access structure and update these as necessary. All the remaining users secret keys will also be updated. Due to the heavy burden of the data owner which may require him to be online at all times to provide key updates, proxy re-encryption is introduced to allow the Cloud to carry out these tasks. Hence most of the computational overhead is delegated to the Cloud. The data owner's data is kept secure and confidential at all times as the Cloud is only exposed to the ciphertext and not the original data contents.

Yang and Zhang [81] also proposed a combination of the ABE scheme and Proxy Re-encryption scheme to enable secure data sharing in the Cloud. The model involves a data owner, say Alice, encrypting data d with a random key k. Alice then determines another random value $k1$ and using access control policy pol, encrypts $k1$ using ABE. Alice then computes $k2$ using operations on k and $k1$, ie, $k2 = k * k1$ and encrypts with her public key using proxy re-encryption. The two keys (ABE key and proxy key) and the encrypted data are then stored in the Cloud. Using an authorisation list, if an authorised user exists, he can then obtain the proxy key which is then

re-encrypted with the user's key. Using this, he decrypts the ABE key, then calculates k, ie, $k1 * k2$ and finally obtains the decrypted file. This technique ensures data is kept confidential against the Cloud and from any unauthorised users. In the scenario that a user is revoked access rights, the data owner simply informs the Cloud to remove that user's entry in the authorisation list and hence is computationally efficient. However, this scheme does not deal with the scenario where a revoked user rejoins the group with different access privileges. The revoked user still has the decryption keys corresponding to ABE and hence in theory can regain access to data he is not allowed to.

Liu et al. [82] proposed a clock-based proxy re-encryption scheme (C-PRE) and combined CP-ABE to achieve fine-grained access control and scalable user revocation. In C-PRE, the data owner and the Cloud share a secret key and this key is used to calculate the PRE keys based on the Cloud's internal clock. The Cloud will re-encrypt the ciphertext with the PRE keys. Each user is associated with a set of attributes and an eligible time which determine how long the user can access the data. The data itself is associated with an access control structure by CP-ABE and also has an access time. When a user requests file access, the Cloud determines the current time using its internal clock and then uses the shared key to calculate PRE keys in time format for all the attributes in the access structure. The PRE keys are then used to re-encrypt the ciphertext. Only users whose attributes satisfy the access control structure and whose eligible time satisfies the access time can decrypt the data. The main benefit with this technique is that the re-encryption of all the data is delegated to the Cloud instead of the data owner and hence is efficient from the data owner's perspective. The user revocation problem is also solved since the data can only be accessed if the user's attribute satisfies the access control structure and their eligible time satisfies the access time. One problem with this technique though, is that data is re-encrypted every time a user makes an access request. Even though the re-encryption is delegated to the Cloud, it is still not a very efficient solution especially when considering very large data sizes.

5.4.4 Discussion

The Table 3 shows a summary of the existing literature based on secure and confidential data sharing in the Cloud. Many of the works reviewed had a strong focus on preventing collusion attacks as well as researching ways for the data owner to be online only when required. In terms of user revocation, some of the reviewed literature showed fast methods of user revocation where revocation involves simply removing a key for instance. Other works required the data to be re-encrypted and the keys to be re-distributed in a secure method and this mainly occurred with works that used ABE techniques.

Data sharing and collaboration in the Cloud is still currently a strong focus of research today and in particular many works are focusing on solving the user revocation problem as well as ways to manage the sharing and collaboration of large data sizes.

Table 3 Summary of literature on secure and confidential data sharing

Method	ABE	PRE	Likelihood of collusion attacks	User revocation	Data owner online all times
Zhao et al. [61]	N	N	N	F	Y
Tu et al. [76]	Y	N	N	S	N
Li et al. [77]	Y	N	N	F	N
Tran et al. [79]	N	Y	Y	F	N
Yu et al. [80]	Y	Y	N	S	N
Yang and Zhang [81]	Y	Y	N	F	N
Liu et al. [82]	Y	Y	N	S	N

Y yes, *N* no, *F* fast, *S* slow

6 Future Directions

In this chapter, we have reviewed literature on ways to provide a secure environment where a data owner can share data with members of his group while preventing any outsiders from gaining any data access in case of malicious activities such as data loss and theft. However, throughout the chapter we assume that members of the group will not carry out malicious activities on the data owner's data.

Auditing and Accountability in the Cloud is a potential for future research in the context of data sharing in the Cloud. As discussed in Sect. 1, many users, in particular organisations and enterprises, benefit from data sharing in the Cloud. However, there is always a likely chance that members of the group can carry out illegal operations on the data such as making illegal copies and distributing copies to friends, general public, etc in order to profit. A future research direction would be to find ways for a data owner to hold accountable any member that carries out malicious activities on their data.

Another research direction would be to give the data owner physical access control over his data. Instead of accountability, the data owner can create a set of access control rules on his data and send the data along with the access control policy. In this way, any member with access to the data can only use the data in such a way that abides by the access control policy. If a member attempts to make illegal copies of the data, the access control policy should "lock" the data to prevent the member from doing so.

Also, since data stored in the Cloud are usually stored and replicated in different geographical locations around the world, it is crucial that the legal jurisdictions are honored and followed. A potential research direction would be to find ways to store and process data in a way that does not breach the privacy and security laws of the region.

7 Summary

Data Sharing and Collobaration in the Cloud is fast becoming available in the near future as demands for data sharing continues to grow rapidly. In this chapter, we presented a review on enabling secure and confidential data sharing and collaboration using Cloud computing technology. We examined definitions related to Cloud computing and privacy. We then looked at privacy and security issues affecting the Cloud followed by what is being done to address these issues.

We then discussed why data sharing in the Cloud is important and the traditional approach to data sharing in the Cloud. We discussed key management in the Cloud and how proper key management leads to more secure and confidential data which can aid secure and private sharing of data in the Cloud. We reviewed current state-of-the-art literature related to key management in the Cloud. We explained the different techniques, namely ABE and PRE that are currently used to enable secure data sharing in the Cloud. We also reviewed current state-of-the-art literature in relation to secure and confidential data sharing in the Cloud and gave a brief overview on the future of data sharing in the Cloud where the data owner could have more control over the usage of their data.

References

1. Mell P, Grance T (2012) The NIST definition of cloud computing. NIST Spec Publ 800:145. National Institute of Standards and Technology, U.S. Department of Commerce. Source: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed on Oct 2012
2. Wikipedia definition of Cloud computing (2012). Source: http://en.wikipedia.org/wiki/Cloud_computing. Accessed on Oct 2012
3. Healey M (2010) Why IT needs to push data sharing efforts. Information Week. Source: http://www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/225700544. Accessed on Oct 2012
4. Gellin A (2012) Facebook's benefits make it worthwhile. Buffalo News.
5. Riley DA (2010) Using google wave and docs for group collaboration. Library Hi Tech News.
6. Wu R (2012) Secure sharing of electronic medical records in cloud computing. Arizona State University, ProQuest Dissertations and Theses
7. Pandey S, Voorsluys W, Niu S, Khandoker A, Buyya R (2012) An autonomic cloud environment for hosting ECG data analysis services. Future Gener Comput Syst 28(1):147–154
8. Bender D (2012) Privacy and security issues in cloud computing. Comput Internet Lawyer 1–15.
9. Judith H, Robin B, Marcia K, Fern H (2009) Cloud computing for dummies. For Dummies.
10. SeongHan S, Kobara K, Imai H (2011) A secure public cloud storage system. International conference on internet technology and secured transactions(ICITST) 2011, pp 103–109.
11. Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and privacy in cloud computing: a survey. Sixth international conferences on emantics knowledge and grid (SKG) 2010:105–112
12. Rocha F, Abreu S, Correia M (2011) The final Frontier: confidentiality and privacy in the cloud, pp 44–50.
13. Huang R, Gui X, Yu S, Zhuang W (2011) Research on privacy-preserving cloud storage framework supporting ciphertext retrieval. International conference on network computing and information security 2011:93–97

14. Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun Surveys Tutorials 99:1–17
15. Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. International conference on computer science and electronics, engineering, pp 647–651.
16. Zhou M (2010) Security and privacy in the cloud: a survey. Sixth international conference on semantics knowledge and grid (SKG) 2010:105–112
17. Wang J, Liu C, Lin GTR (2011) How to manage information security in cloud, computing, pp 1405–1410.
18. Wang Y (2011) The role of SaaS privacy and security compliance for continued SaaS use. International conference on networked computing and advanced information management (NCM) 2011:303–306
19. Oza N, Karppinen K, Savola R (2010) User experience and security in the cloud-An empirical study in the finnish cloud consortium. IEEE second international conference on cloud computing technology and science (CloudCom) 2010:621–628
20. Sarathy R, Muralidhar K (2006) Secure and useful data sharing. Decis Support Syst 204–220.
21. Butler D Data sharing threatens privacy, vol 449(7163). Nature Publishing, Group, pp 644–645.
22. Mitchley M (2006) Data sharing: progress or not? Credit, Manage 10–11.
23. Feldman L, Patel D, Ortmann L, Robinson K, Popovic T (2012) Educating for the future: another important benefit of data sharing. Lancet 1877–1878.
24. Geoghegan S (2012) The latest on data sharing and secure cloud computing. Law, Order 24–26.
25. Sahafizadeh E, Parsa S (2010) Survey on access control models. 2nd international conference future computer and communication (ICFCC) 2010, pp V1–1-V1-3.
26. Parker RB (1973) A definition of privacy. Rutgers Law Rev 275.
27. Schwab AP, Frank L, Gligorov N (2011) Saying privacy, meaning confidentiality. Am J Bioeth 44–45.
28. HIPAA Privacy (2012) U.S. Department of Health and Human Services. Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html. Accessed on Nov 2012
29. Internet privacy? (2001) School Libraries in Canada 20–22.
30. Donlon-Cotton C (2010) Privacy and social networking. Law, Order 16–17.
31. Priscilla MR (1986) Privacy, government information, and technology. Public Admin Rev 629–634. Source: http://www.jstor.org/stable/976229. Accessed on Oct 2012
32. Federal Privacy Act. About.com Source: http://usgovinfo.about.com/library/weekly/aa121299a.htm. Accessed on Oct 2012
33. Mcbeth J (2011) Governments need privacy too. The Straits Times.
34. WikiLeaks. Source: http://wikileaks.org. Accessed on Oct 2012
35. Verma R (2012) Confidentiality and privacy issues. The Law Handbook. Education Law. Source: http://www.lawhandbook.org.au/handbook/ch06s03s08.php. Accessed on Oct 2012
36. Ruhr (2011) Cloud computing: Gaps in the 'cloud'. NewsRx Health Sci.
37. Zunnurhain K, Vrbsky SV (2010) Security attacks and solutions in clouds. CloudCom2010 Poster.
38. Motivations of a Criminal Hacker. Microsoft TechNet. Source: http://technet.microsoft.com/en-us/library/cc505924.aspx. Accessed on Oct 2012
39. Hacking Attacks-How and Why. Crucial Paradigm Web Solutions. Source: http://www.crucialp.com/resources/tutorials/website-web-page-site-optimization/hacking-attacks-how-and-why.php
40. Andy P (2007) Salesforce.com Scrambles To Halt Phishing Attacks. http://InternetNews.com. Accessed on Oct 2012
41. Charles A (2011) PlayStation Network: hackers claim to have 2.2m credit cards. The Guardian Technology Blog. Source: http://www.guardian.co.uk/technology/blog/2011/apr/29/playstation-network-hackers-credit-cards. Accessed on Oct 2012
42. Whitney L (2011) Feds investigate alleged attacks on Gmail accounts. CNet news. Source: http://news.cnet.com/8301-1009_3-20068229-83/feds-investigate-alleged-attacks-on-gmail-accounts. Accessed on Oct 2012

43. Jim C, Chyen Yee L (2011) Hacker attacks threaten to dampen cloud computing's prospects. Reuters article. Source: http://www.reuters.com/article/2011/06/03/us-cloudcomputing-idUSTRE7521WQ20110603. Accessed on Oct 2012
44. Dominguez K (2012) Trend micro researchers identify vulnerability in hotmail. Trend Micro. Source: http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-researchers-identify-vulnerability-in-hotmail/. Accessed on Oct 2012
45. Choney S (2011) Hotmail, Yahoo Mail users also targets in attacks. NBC News. Source: http://www.nbcnews.com/technology/technolog/hotmail-yahoo-mail-users-also-targets-attacks-123078. Accessed on Oct 2012
46. Galvin N (2012) File-sharing service users in cloud over access to data. The Age.
47. Hulme G (2009) Amazon web services DDoS attack and the cloud. InformationWeek. Source: http://www.informationweek.com/security/amazon-web-services-ddos-attack-and-the/229204417. Accessed on Oct 2012
48. Hachman M (2012) New facebook phishing attack steals accounts, financial information. PC Mag. Source: http://www.pcmag.com/article2/0,2817,2398922,00.asp. Accessed on Oct 2012
49. Albanesius C (2012) Ramnit computer worm compromises 45K facebook logins. PC Mag. Source: http://www.pcmag.com/article2/0,2817,2398432,00.asp. Accessed on Oct 2012
50. NIST Privacy and Security guideslines (2012) NIST. Source: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf. Accessed on Oct 2012
51. Cavoukian A (2008) Privacy in the clouds. Identity Inf Soc 1(1):89–108
52. Sabahi F (2011) Cloud computing security threats and responses. IEEE 3rd international conference communication software and networks (ICCSN) 2011, pp 245–249.
53. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y (2010) Fine-grained data access control systems with user accountability in cloud computing. IEEE second international conference on cloud computing technology and science(CloudCom) 2010, pp 89–96.
54. Naone E (2011) Homomorphic encryption. Technol Rev 50–51.
55. Yao J, Chen S, Nepal S, Levy D, Zic J (2010) TrustStore: making Amazon S3 trustworthy with services composition. 10th IEEE/ACM international conference cluster, cloud and grid computing (CCGrid) 2010, pp 600–605.
56. Scale ME (2009) Cloud computing and collaboration. Library Hi Tech News, pp 10–13.
57. Ratley N (2012) Data-sharing 'would benefit patients'. The Southland Times.
58. Melis RJF, Vehof H, Baars L, Rietveld MC (2011) Sharing of research data. Lancet 378(9808):1995
59. Feldman L, Patel D, Ortmann L, Robinson K, Popovic T (2012) Educating for the future: another important benefit of data sharing. Lancet 379(9829):1877–1878
60. What's in it for me? the benefits of sharing credit data (2011). Banker, Middle East.
61. Zhao G, Rong C, Li J, Zhang F, Tang Y (2010) Trusted data sharing over untrusted cloud storage providers. IEEE second international conference cloud computing technology and science(CloudCom) 2010, pp 97–103.
62. Luther M (2010) Federated key management for secure cloud computing. Voltage security conference presentation. Source: http://storageconference.org/2010/Presentations/KMS/17.Martin.pdf. Accessed on Nov 2012
63. Pate S, Tambay T (2011) Securing the Cloud-Using encryption and key management to solve today's cloud security challenges. Storage Networking Industry Association 2011. Source: http://www.snia.org/sites/default/education/tutorials/2011/spring/security/PateTambay_Securing_the_Cloud_Key_Mgt.pdf. Accessed on Nov 2012
64. Encryption and Key Management (2012) Cloud security alliance wiki. Source: https://wiki.cloudsecurityalliance.org/guidance/index.php/Encryption_and_Key_Management. Accessed on Nov 2012
65. Mather T (2010) Key management in the cloud. O'Reilly Community. Source: http://broadcast.oreilly.com/2010/01/key-management-in-the-cloud.html. Accessed on Nov 2012
66. OASIS Key Management Interoperability Protocol (2012) Web site. Source: https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=kmip#overview. Accessed on Nov 2012

67. Key Management Interoperability Protocol (2012) Wikipedia definition. http://en.wikipedia.org/wiki/Key_Management_Interoperability_Protocol. Accessed on Nov 2012
68. Barker E, Barker W, Burr W, Polk W, Smid M (2007) Recommendation for key management-Part 1: general (Revised). Computer Security. NIST Spec Publ 800–857. Source: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf. Accessed on Nov 2012
69. ISO/IEC 11770–5:2011 Information technology-Security techniques-Key management-Part 5: group key management. ISO Standards catalogue. Source: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54527. Accessed on Nov 2012
70. ISO 11568–2:2012 Financial services - Key management (retail) - Part 2: Symmetric ciphers, their key management and life cycle. ISO Standards catalogue. Source: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53568. Accessed on Nov 2012
71. Lei S, Zishan D, Jindi G (2010) Research on key management infrastructure in cloud computing environment. 9th international conference on grid and cooperative computing (GCC) 2010, pp 404–407.
72. Fathi H, Shin S, Kobara K, Chakraborty S, Imai H, Prasad R (2006) LR-AKE-based AAA for network mobility (NEMO) over wireless links. IEEE J Select Areas Commun 24(9):1725–1737
73. Sanka S, Hota C, Rajarajan M (2010) Secure data access in cloud computing. IEEE 4th international conference internet multimedia services architecture and application(IMSAA) 2010, pp 1–6.
74. Bennani N, Damiani E, Cimato S (2010) Toward cloud-based key management for outsourced databases. IEEE 34th annual computer software and applications conference workshops (COMPSACW) 2010, pp 232–236.
75. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on computer and communications security (CCS '06) 2006, pp 89–98.
76. Tu S, Niu S, Li H, Xiao-ming Y, Li M (2012): Fine-grained access control and revocation for sharing data on clouds. IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.
77. Li M, Yu S, Zheng Y, Ren K, Lou W (2013) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst 131–143.
78. Wang X, Zhong W (2010) A new identity based proxy re-encryption scheme. International conference biomedical engineering and computer science (ICBECS) 2010:145–153
79. Tran DH, Nguyen HL, Zha W, Ng WK (2011) Towards security in sharing data on cloud-based social networks. 8th International conference on information, communications and signal processing (ICICS) 2011, pp 1–5.
80. Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM, 2010 proceedings IEEE, pp 1–9
81. Yang Y, Zhang Y (2011) A generic scheme for secure ata sharing in cloud. 40th international conference parallel processing workshops (ICPPW) 2011, pp 145–153.
82. Liu Q, Wang G, Wu J (2012) Check-based proxy re-encryption scheme in unreliable clouds. 41st international conference on parallel processing workshops (ICPPW) 2012, pp 304–305.

http://www.springer.com/978-3-642-38585-8

Security, Privacy and Trust in Cloud Systems
Nepal, S.; Pathan, M. (Eds.)
2014, XX, 459 p. 146 illus., 95 illus. in color., Hardcover
ISBN: 978-3-642-38585-8