

A New Model to Ensure Security in Cloud Computing Services

Mohammed A. AlZain, Ben Soh, Eric Pardede

Received: 21 February 2012 / Accepted: 31 May 2012 / Published: 30 June 2012

© The Society of Service Science and Springer 2012

ABSTRACT

In the commercial world, various computing needs are provided as a service. Service providers meet these computing needs in different ways, for example, by maintaining software or purchasing expensive hardware. Security is one of the most critical aspects in a cloud computing environment due to the sensitivity and importance of information stored in the cloud. The risk of malicious insiders in the cloud and the failure of cloud services have received a great deal of attention by companies. This paper focuses on issues related to data security and privacy in cloud computing and proposes a new model, called Multi-Cloud Databases (MCDB). The purpose of the proposed new model is to address security and privacy risks in the cloud computing environment. Three security issues will be examined in our proposed model: data integrity, data intrusion, and service availability.

KEYWORDS

Cloud Computing, Single Cloud, Multi-Clouds, Cloud Storage, Data Integrity, Data Intrusion, Service Availability.

Mohammed A. AlZain (✉)

PhD Candidate, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora, 3086, Australia.
e-mail: maalzain@students.latrobe.edu.au, alzain50@hotmail.com

Ben Soh

Associate Professor, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.
e-mail: b.soh@latrobe.edu.au

Eric Pardede

Ph.D, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.
e-mail: e.pardede@latrobe.edu.au

1. INTRODUCTION

In any organization, the use of technology to store, evaluate, and process data in databases is extremely significant. Consequently, organizations have to translate data into meaningful information to help them improve their decision making or create strategic advantages (Lee et al. 2002). The need for data outsourcing or database as a service (DaaS) is increasingly important for many organizations. The use of cloud computing has also increased rapidly and offers many advantages, such as fast access to applications or a decrease in infrastructure costs (Subashini and Kavitha 2011).

The security of cloud computing is the most critical issue in the cloud computing environment due to the valuable information which users store in the cloud. Cloud providers should address privacy and security issues as a matter of high and urgent priority (BNA). Due to the importance of data security in cloud computing, this paper focuses on issues related to the security aspects of cloud computing. It proposes a Multi-cloud Database Model (MCDB) which uses multiple cloud service providers instead of a single cloud service provider, such as the Amazon cloud service (Amazon 2010). The purpose of the new model is to address security and privacy risks in the cloud computing environment. Three security issues will be examined in our proposed model: data integrity, data intrusion, and service availability.

The remainder of this paper is organized as follows. Section 2 discusses examples of single cloud service providers. In addition, it presents Shamir's secret sharing algorithm which will be used in our proposed model. Section 3 describes the security risks in cloud computing and recommends a move towards multi-clouds. Section 4 describes the proposed new model, called MCDB, with a thorough data flow explanation. Section 5 discusses the analysis and implementation of the proposed model. Section 6 concludes the paper with suggestions for future work.

2. RELATED WORK

This section presents examples of single clouds as a comparison to our proposed model. In addition, it explains Shamir's secret sharing algorithm which will be used in our proposed model.

2.1 Cloud Computing: Preliminary

(Takabi et al. 2010) describe cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Cloud computing consists of three components: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The Amazon web service (Kamara and Lauter 2010) is an example of IaaS, Google Apps is an example of PaaS and the Salesforce.com CRM application (Subashini and Kavitha 2011, Takabi et al. 2010) is an example of SaaS.

2.2 Single Cloud Providers

In the commercial world, various computing needs are provided as a service. Service providers meet these computing needs in different ways, for example, by maintaining software or purchasing expensive hardware. For instance, the service EC2, created by Amazon, provides customers with scalable servers. As another example, under the CLuE program, NSF joined with Google and IBM to offer academic institutions access to a large-scale distributed infrastructure (Agrawal et al. 2009).

There are many features of cloud computing. Firstly, cloud storage services such as Amazon S3, Microsoft SkyDrive, or Nirvanix CCloudNAS allow consumers to access their data online. Secondly, it provides computation resources for users such as those provided by Amazon EC2. Thirdly, Google Apps or versioning repositories for source code are examples of online collaboration tools (Cachin et al. 2009).

Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure. A cloud provider offers many services that can benefit its customers such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and the use of network and infrastructure facilities (Subashini and Kavitha 2011).

Amazon EC2 also supports the building of a cloud computing environment as a group of virtual machines, which is known as virtualization technology. Supporters of this technology

argue that software and hardware for this computational environment are compatible with each other and users do not need to perform compatibility measures between them. Opponents of this methodology argue about the overheads of virtual machines and the negative aspects of sharing one physical machine with other virtual machines (Akioka and Muraoka 2010).

In the cloud computing environment, Amazon EC2 is a collection of virtual machine nodes or instances. In relation to the users' charges for Amazon EC2, the communication between instances and communication between instances and machines outside Amazon EC2 will be charged based on CPU time (Amazon 2010). Kaufman (2009) developed a security model that ensures data confidentiality, data integrity, and data availability (CIA). The cloud storage provider must be able to provide an encryption schema for the stored data, access control for their data to prevent an unauthorized user from accessing the data, and provide a backup service for their data.

2.3 Shamir's Algorithm

In previous research (AlZain and Pardede 2011), we proposed a new model called NetDB2 Multi-Shares (NetDB2-MS). NetDB2-MS ensures privacy in DaaS and is based on data distribution in different service providers (Agrawal et al. 2009). In addition, it also employs Shamir's secret sharing algorithm (Shamir 1979).

Agrawal et al. (2009) discussed the issue of information distribution with the aim of showing that there is an orthogonal approach which is based on information distribution instead of encryption in the area of data and computer security. The need to communicate important or private information from one party to another instigated most of the work on data security.

Agrawal et al. (2009) introduced Shamir's secret sharing algorithm (Shamir 1979) as a solution for the privacy issue. The algorithm proposed dividing the data D into (n) pieces (D_1, \dots, D_n) in such a way that knowledge of any k or more of D_i pieces makes the value of D known. Therefore, a complete knowledge of $(k-1)$ pieces reveals no information about D and k should be less than n to keep the value of shares unconstructible and ensure that an adversary cannot access k data pieces. Shamir's method theoretically secures information.

In addition, by using a (k, n) threshold scheme with $n = 2k-1$, Agrawal et al. (2009) show

that a strong key management scheme can be achieved. The goal is to take a distributed approach to secure DaaS, the reason being that they want to explore the use of a secret-sharing approach and multiple service providers. The advantage of this approach is that it addresses both privacy-preserving querying and the security of outsourced data (AlZain and Pardede 2011).

2.3.1 Overview of the Secret-Sharing Approach

Instead of encryption techniques, the secret-sharing method (Agrawal et al. 2009) distributes data to multiple servers to ensure the privacy of user queries. If the client wants to outsource the data from data source D to database service providers (DAS_1, \dots, DAS_n), data should be divided into n shares and each share should be stored in a different DAS. Any query from a client to D will be sent to all DASs to retrieve the relevant shares without revealing the value of data shares from the service provider.

In order to reconstruct the secret value v_s at the data source, the knowledge of any k can refer to v_s besides some secret information X that is known only to the data source. Therefore, even with a full knowledge of $(k-1)$, DAS will not be able to determine the value of v_s even if X is known to them (Na et al. 2001). Furthermore, D chooses a random polynomial $q(x)$ of degree $(k-1)$, where the constant is v_s . Each DAS has v_s as well as X which is a set of n random points for each respective DAS. Figure 1 illustrates how the shares can be written (Agrawal et al. 2009). In Figure 1, a and b are the coefficient values of the polynomial $q(x)$.

Shares ($v_s, 1$) = $q(x_1) = ax_1^{k-1} + bx_1^{k-2} \dots + v_s$
Shares ($v_s, 2$) = $q(x_2) = ax_2^{k-1} + bx_2^{k-2} \dots + v_s$
\vdots
Shares (v_s, n) = $q(x_n) = ax_n^{k-1} + bx_n^{k-2} \dots + v_s$

Figure 1. Example of Shares Using Polynomial Function (Agrawal et al. 2009)

Figure 2 shows an example of data source D that has *EMPLOYEE* table and *SALARY* attribute. D wants to outsource the *SALARY* to three DASs (DAS_1, DAS_2 , and DAS_3). In addition, D chooses 5 random polynomials with a degree of one (this is for each *SALARY*). Since the number of shares $n = 3$, $k = 2$ and the secret information $X \{x_1 = 2, x_2 = 4, \text{ and } x_3 = 1\}$ will be used by the polynomial functions for distribution to each DAS. In other words, the

value of x in DAS_1 will be ($x_1 = 2$), DAS_2 will be ($x_2 = 4$), and in DAS_3 will be ($x_3 = 1$).

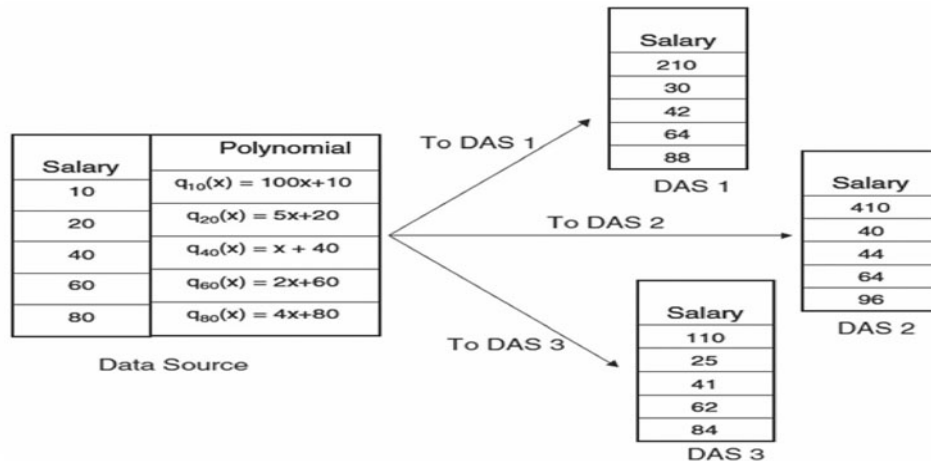


Figure 2. Data Distribution in Multiple DASs (Agrawal et al. 2009)

Agrawal et al. (2009) extend the approach to retrieve the required data from the service provider instead of retrieving all the shares and thus decreases the cost of communication and computation in the processing of the query. They achieved this by constructing order-preserving polynomials with polynomial functions and sending them to each DAS to retrieve any value later, according to its order.

3. CLOUD COMPUTING SECURITY

This section discusses the security risks of cloud computing. In addition, it advocates movement from a single cloud to multi-clouds.

3.1 Security Risks

As discussed earlier, cloud service providers can offer benefits to users, but security risks play a major role in the cloud computing environment (Viega 2009). Users who use online data sharing or network facilities are aware of the potential loss of privacy (Cachin et al. 2009). According to a recent IDC survey (Clavister 2008), 74% of IT executives and CIOs stated that security was the issue of greatest concern in the cloud computing environment. Protecting private and important information such as credit card details or patients' medical

records from attackers or malicious insiders is of critical importance (Mei et al. 2009). Moving databases to large data centers involves many security challenges (Wang et al. 2009) such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Subashini and Kavitha (2011) discuss several fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources.

In different cloud service models, the security responsibility between users and providers is different. According to Amazon (Seccombe 2009), their EC2 addresses physical, environmental and virtualization security, whereas the users remain responsible for addressing the security of the IT system, including the operating systems, applications and data. (Ristenpart et al. 2009) claim that the levels of security issues in IaaS are different. Naturally, the impact of security issues in a public cloud is greater than the impact in a private cloud.

As cloud services have been built over the internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the internet; consequently, even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through the network, which may be insecure. As a result, the impact of internet security problems will affect the cloud. Moreover, cloud risks are even more dangerous when the resources stored within them are valuable and the cloud is vulnerable. The technology used in the cloud is similar to the technology used on the internet. Encryption techniques and secure protocols are not sufficient to assist data transmission in the cloud. Data intrusion of the cloud through the internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients (Subashini and Kavitha 2011).

3.2 Why Move to Multi-Clouds?

The migration of cloud computing from a single cloud to multi-clouds to ensure the security of user's data is extremely important (AlZain et al. 2012). The term "multi-clouds" is similar to the terms "intercloud" or "cloud-of-clouds" that were introduced by Vukolic (2010). This work suggests that cloud computing should not end with a single cloud. Using

their illustration, a cloudy sky incorporates different colors and shapes of clouds which leads to different implementations and administrative domains.

Recent research has focused on the multi-cloud environment (Abu-Libdeh et al. 2010, Bessani et al. 2011, Bowers et al. 2009, Cachin et al. 2010) which controls several clouds and avoids dependency on any one individual cloud. Moving from a single cloud or inner-cloud to multi-clouds is a logical decision for many reasons. According to Cachin et al. (2009) “services of single clouds are still subject to outage.” In addition, (Bowers et al. 2009) showed that over 80% of company management “fear security threats and loss of control of data and systems.” (Vukolic 2010) assumes that the main purpose of moving to an intercloud is to improve what is offered in a single cloud by distributing reliability, trust and security among multiple cloud providers. Furthermore, reliable distributed storage (Chockler et al. 2009) which utilizes a subset of Byzantine fault tolerance (BFT) techniques has been suggested by Vukolic (2010) for use in multi-clouds. A number of recent studies in this area have built protocols for interclouds (Abu-Libdeh et al. 2010, Bessani et al. 2011, Bowers et al. 2009, Cachin et al. 2010).

4. PROPOSED MODEL

In this section, we propose a new model called the Multi-cloud Database (MCDB). The purpose of the proposed model is to avoid the risk of malicious insiders in the cloud and to avoid the failure of cloud services. Security risks such as data integrity, data intrusion, and service availability will be examined in the model.

MCDB ensures security and privacy in cloud service providers (CSP) and is based on multi-clouds and the secret sharing algorithm. These techniques have been used in previous database security research (AlZain and Pardede 2011). MCDB provides “cloud database” which gives customers with different types of database queries, such as aggregation, exact match and range query, the ability to store different types of data.

4.1 Multi-Cloud Database Model

Figure 3 gives a general overview of the cloud computing environment. Part A represents the client side, which sends data inquiries to servers or instances in the cloud service provider

in part B. The data source in part B stores the data in the cloud side which is supposed to be a trusted cloud. In addition, the privacy of any query the client has made must be maintained. But one cannot guarantee the cloud provides a trusted service.

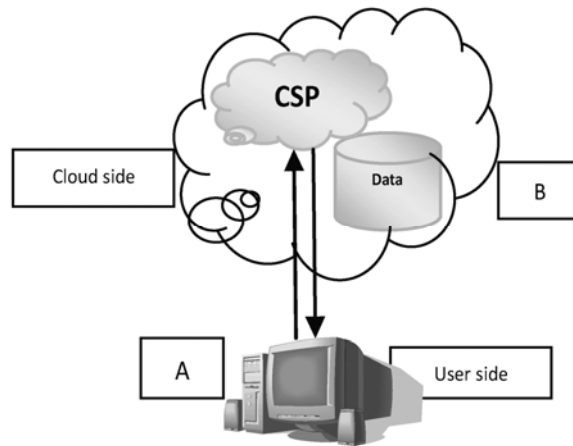


Figure 3. General Overview of User/Cloud Model

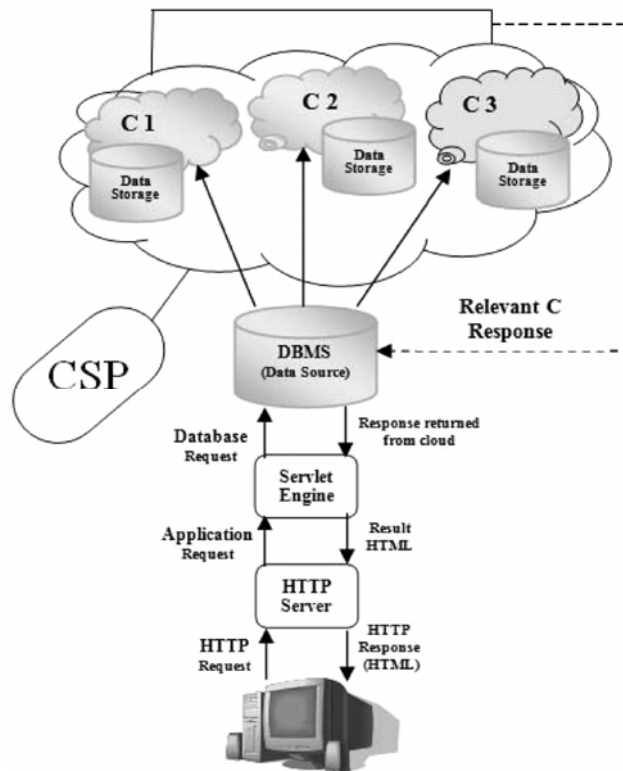




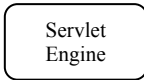
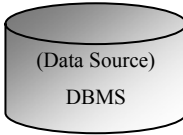
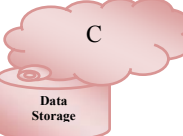
Figure 4. General Overview of Multi-Clouds

MCDB provides database storage in multi-clouds which is different to the Amazon cloud service. The MCDB model (see Figure 4) does not preserve security by using a single cloud; rather the security and privacy of data is preserved by applying the multi-share technique (AlZain and Pardede 2011) on multi-clouds. In doing so, the negative consequences of using a single cloud are avoided, reducing security risks from malicious insiders in the cloud computing environment, and reducing the negative impact of encryption techniques.

MCDB preserves the security and privacy of a user's data by replicating data among several clouds and by using the secret sharing approach. It uses the database management system DBMS (data source) to manage and control the operations between the clients and the multi-clouds inside a cloud service provider.

Table 1 describes each component in the proposed model. Data is divided depending on the number of clouds (C), which is the main factor in the secret sharing approach.

Table 1. Description for MCDB Components



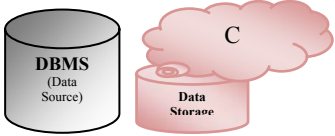
Component	Description
	End user's web browser is responsible for displaying the user interface.
	HTTP server is responsible for managing the communication between the application and the browser. The user interface is generated by the execution from the application for server side logic.
	The Servlet Engine communicates with the data source through the JDBC protocol.
	DBMS is responsible for rewriting the user's query (one for each C), generating polynomial values (polynomial values are not stored at the data source but are generated at the data source at the beginning and end of query processing), handling the user's query to each C and then receiving the result from C.
	C is responsible for storing the data in its cloud storage (like S3 in Amazon), that is divided into n shares and then returning the relevant shares to the DBMS that consists of the user's query result.

4.2 The MCDB Layers

MCDB contains three layers (Table 2): the presentation layer, the application layer, and

the data management layer. The presentation layer contains the end user’s browser and HTTP server. The management layer consists of the Database Management System (DBMS) and the database service provider. DBMS communicates with the Servlet Engine through the JDBC protocol. Communication between components is through a secured private high speed network that uses secure protocols.

Table 2. MCDB Layer

Layer Name	Component
Presentation Layer	
Application Layer	
Management Layer	

4.3 The MCDB Model Data Flow

This section will discuss the data flow for the MCDB model and shows the procedure for sending the data to the DBMS and how the users can run queries through the model in a secure and private way. In addition, it describes how DBMS manages the data and divides them into shares and distributes shares into different clouds (C) inside a cloud service provider.

4.3.1 Sending Data Procedure

As shown in Figure 4, a user sends a query by using a user interface and a web browser through an HTTP request. The HTTP server plays a major role in communication between the web browser and the application. The user’s query will be sent from the HTTP server to a Servlet Engine by an application request. Hereafter, the communication between the Servlet Engine and the DBMS is done by a JDBC protocol. When the query arrives at the data source, the DBMS will manage the query and send it to the C. After the result of the query is returned to the DBMS, the DBMS returns the query result to the Servlet Engine and then the

HTTP server returns the result of the query to the user interface again. The benefit for the HTTP server is the communication between the two components: the user browser and the Servlet Engine.

4.3.2 Procedure between DBMS and C

We extend Shamir's secret sharing approach to suit our MCDB model. In this section, we describe the data flow from DBMS to the multi-clouds inside a cloud service provider in our proposed model MCDB. DBMS divides the data into n shares and stores each share in a different C (see Figure 5). After that, the DBMS generates a random polynomials function in the same degree for each value of the attribute that the client wants to hide from the untrusted cloud provider. The polynomials are not stored at the data source but are generated at the front (when the query received from user at DBMS) and the end of the query processing (when the value is retrieved from C) at the data source. When a user's query arrives at the DBMS, the DBMS rewrites n queries, one query for each C and there are n C s. After this, the relevant share will be retrieved from the C . For example, the rewritten query for C_1 retrieves all workers whose salary is *share* (2000, 1) where the secret value is the salary 2000 and the cloud order is C_1 . To find *share* (2000, 1), data source D first generates polynomials for the secret value salary 2000 and the position for the value in the share $q_{2000}^{(xi)}$. After retrieving the relevant tuple from C , D computes the secret value to send to the client through a secured and private network. The secret sharing method can be applied to execute different types of queries such as exact match, range, and aggregation query.

5. ANALYSIS AND IMPLEMENTATION

This section discusses two issues: firstly, it describes the MCDB scenario and the working of its components as well as explaining the data storage and retrieval procedure in our proposed model; secondly, it analyzes and compares the proposed MCDB model and the Amazon cloud service model in terms of data integrity, data intrusion and service availability.

5.1 MCDB Scenario

In our proposed model, DBMS divides the data that the user wants to hide from the

untrusted cloud provider into n shares or clusters. After dividing the data (assuming the data is a numeric value, for example, a worker's salary) into 3 shares and storing them in different Cs, the DBMS generates random polynomial functions with a degree at the same level, one for each worker's salary in the WORKER table with the actual salary as the constant part of the function. These values will then be stored in different Cs. For this scenario, the value of $n = 3$ and $k = 2$. Note: $n = 2k-1$ (see section 2). In addition, the DBMS uses the secret information X values ($x_1 = 3, x_2 = 1, x_3 = 2$) to create the secret value. The polynomial for salaries {1000, 2500, 2900, 3000, and 3200} would be: $q_{1000}(x) = 100x+1000$; $q_{2500}(x) = 5x + 2500$; $q_{2900}(x) = x+2900$; $q_{3000}(x) = 2x+3000$; and $q_{3200}(x) = 4x+3200$. If x_1 is applied in polynomials, the value of salary 1000 will be stored as 1300 at C_1 and stored as 1100 at C_2 and stored as 1200 at C_3 .

For data retrieval, at this stage, the user's query should have arrived at the DBMS and the DBMS should have rewritten the query again to retrieve the result from the relevant share from C. Then, the DBMS computes the secret value and sends it to the client.

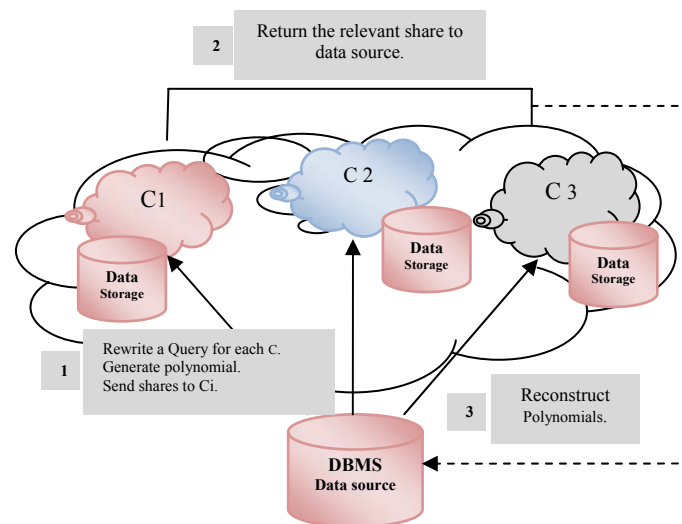


Figure 5. Procedure between DBMS/C

The numeric attribute data type is considered in the secret sharing approach. Therefore, to represent a non-numeric attribute data type, we converted the non-numeric attribute into a numeric attribute by applying a converted attribute to the schema. In other words, any word

consists of 27 possible characters which are enumerated ($*$ = 0, A = 1, B = 2, C = 3, ..., Z = 26). In our scenario, if the user wants to query the suburb for a certain worker living in “Reservoir”, the value of the address will be converted to a numeric value as (185195182 215918) and will execute the polynomial functions on this value before it is stored in C.

5.1.1 Data storing procedure

Data storage in MCDB involves data distribution from the data source to different clouds inside CSP. This is done after executing the polynomial functions on the data. On the other hand, the Amazon cloud service asks the organization to encrypt their data before storing it in their instances. As a comparison between Amazon and MCDB in relation to data storage time, our proposed model is similar to cluster computing. Therefore, obviously the multi-clouds will suffer in terms of time and cost. This does not affect our contribution to ensuring the privacy of users’ queries during the data retrieval process.

To analyse the effect of the number of shares in our model, we perform experimentation written in Java for data storage in MCDB, using a static data size (10 MB). Figure 6 shows that the time cost for the data storage procedure increases with the number of shares. Even though the time cost is increased along with the increased number of shares, increasing the number of shares will improve the security level of the hidden value of the data from an untrusted cloud due to the fact that the malicious insiders in Cs will need a greater number of k to know the details of the data. If the number of shares decreases to fewer than 3, then it might not be very effective for privacy purposes.

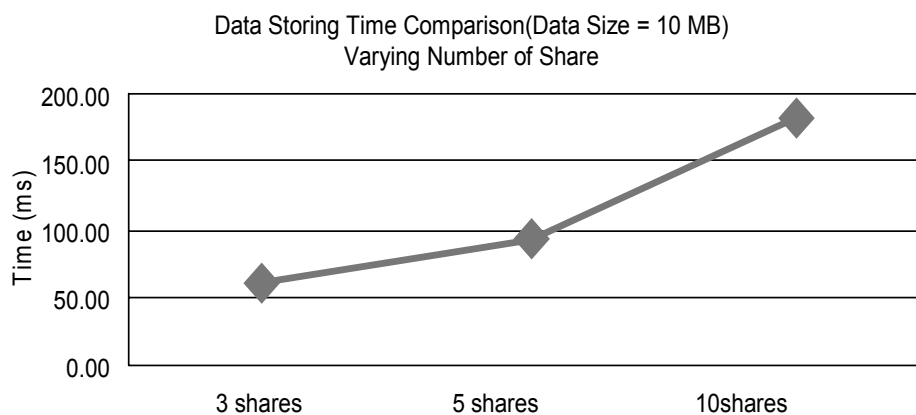


Figure 6. Data Storage Time Comparison, Varying the number of Shares

5.1.2 Data Retrieval Procedure

The data retrieval process in the MCDB model starts with rewriting the user's query in the DBMS (n numbers of queries) and then sending these queries, one for each C , after constructing the polynomial and the order for the secret value. The relevant tuple will be returned to the DBMS to compute the polynomial function on the returned value. On the other hand, data retrieval in the Amazon cloud service focuses on data decryption after the data has been retrieved from their instances.

As an evaluation for the outcomes of data retrieval for various numbers of shares in the secret sharing algorithm in MCDB model, Figure 7 shows that data retrieval time increases linearly with an increased number of shares. On the other hand, we argue that increasing the number of shares will also increase the security level of data because the malicious insiders in C_s will need to retrieve more values from more shares in order to be able to determine the hidden information in C_s .

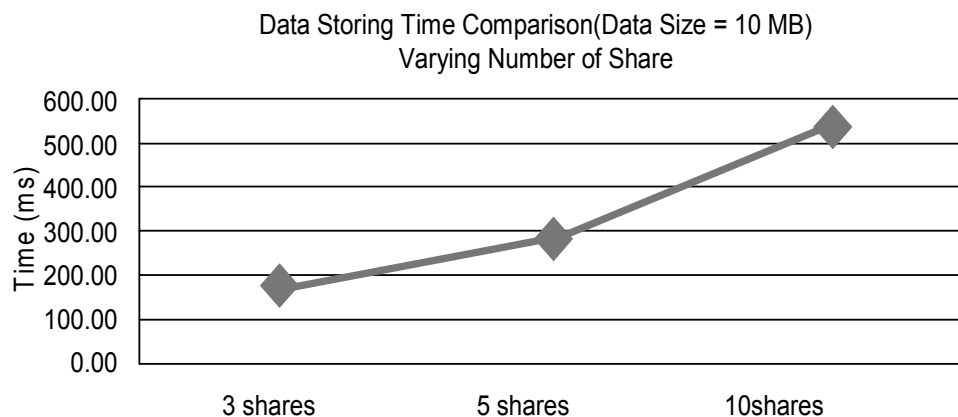


Figure 7. Data Retrieval Time Comparison, Varying the number of Shares

5.2 What Makes MCDB Different?

The security of our proposed MCDB model differs from the Amazon cloud service in the following three ways:

5.2.1 Data Integrity

One of the most important issues relating to cloud security risks is data integrity. The

stored data in the cloud may suffer from damage occurring during transition operations from or to the cloud storage provider. The risk of attacks from both inside and outside the cloud provider should be taken seriously. For example, data integrity was recently compromised in Amazon S3 where users suffered from data corruption (Sun). Garfinkel (2007) argues that information privacy is not guaranteed in Amazon S3. Data authentication assures that the returned data is the same stored data, which is extremely important. Garfinkel claims that instead of following Amazon's advice that organizations encrypt data before storing them in Amazon S3, organizations should use HMAC (Krawczyk et al. 1997) technology or a digital signature to ensure data is not modified by Amazon S3. These technologies protect users from data modification by Amazon and from hackers who may have obtained access to their email or have stolen their password (Garfinkel 2007).

However, as previously explained, the proposed MCDB model uses multi-clouds which is different from the Amazon cloud service. In addition, the use of Shamir's secret approach is another point of difference with MCDB. For example, data will be distributed into three different clouds inside one CSP in the proposed MCDB model. In addition, the secret sharing algorithm will be applied on the stored data in the multiple clouds. If an intruder or malicious insider wants to know the hidden information inside the cloud, they need to retrieve at least three values from three different clouds to be able to know the real value which has been converted and hidden before being stored in the multi-clouds.

This approach depends on Shamir's secret sharing algorithm with a polynomial function technique which states that, if there are 3 shares stored in 3 clouds ($n = 3$, $k = 2$), the knowledge of the value of 2 shares or less makes the secret unconstructible, whereas knowledge of the values of more than two shares will enable the value to be reconstructed. Therefore, the MCDB model is superior to the Amazon cloud service in addressing the issue of data integrity.

5.2.2 Data Intrusion

According to Garfinkel (2007), another security risk that may occur with a cloud provider such as Amazon, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and

resources. In addition, the stolen password allows the hacker to erase all the information inside the instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility that the user's email account (Amazon user name) can be hacked (see Garfinkel 2003) for a discussion of the potential risks of E-mail). Since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

However, the MCDB model is different from the Amazon cloud service model. As MCDB replicates the data among three different clouds, hackers need to retrieve all the information from the three clouds to be able to reconstruct the real value of the data in the cloud. In other words, if a hacker manages to hack the cloud's password or even two clouds' passwords, they still need to hack the third cloud (in our case) to know the secret, which is the worst case scenario and the most difficult to achieve. Hence, replicating data into multi-clouds by using a multi-share technique (AlZain and Pardede 2011), as in the MCDB model, may reduce the risk of data intrusion and is a point of difference between the MCDB model and the Amazon single cloud.

5.2.3 Service Availability

Another major concern in cloud services is service availability. Amazon (Amazon 2006) mentions in its licensing agreement that there is a possibility of the service being unavailable from time to time. Also, the user's web service may be terminated for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to Amazon's web service and the service fails, there will be no compensation from the Amazon Company regarding this failure. In order to avoid system failure in the event of the cloud provider's service being unavailable, companies protect their data with backups or disconnection to any dependent cloud providers (Garfinkel 2007). However, MCDB is different from the Amazon cloud service in relation to service availability risk or loss of data. MCDB distributes the data into different clouds, therefore it could be argued that the risk of losing data is reduced. If one cloud fails, users can still access their data live in other clouds.

According to other research, to ensure backup even if instances are down Garfinkel (2007) suggested running services on multiple instances in Amazon EC2 and storing data in multiple

Amazon S3, then linking different Amazon Web Services (AWS) to different email addresses used as a user name. However, there would be a dilemma if, for example, Amazon decided to delete the user's data for any reason from their all instances, depending on their web service licensing agreement (WSLA)(Amazon 2010). Therefore, using multi-clouds in the MCDB model may reduce the risk of loss of data.

In light of the three arguments above on data integrity, data intrusion, and service availability, our proposed MCDB model is better in addressing the three security issues than the Amazon cloud service provider. In addition, our proposed model is more secure in terms of protecting the user's data from untrusted cloud service providers and from malicious insiders. The Amazon cloud service asks users to encrypt their data before storing it in their instances, whereas MCDB takes responsibility for this task.

Table 3 summarizes the differences between Amazon and our proposed MCDB model in terms of the three security issues that may occur in the cloud computing environment.

Table 3. Comparison between Amazon/MCDB

	Data Integrity	Data Intrusion	Service Availability	Data Status	
				safe	Lost
Amazon	If data hacked?	If password hacked?	If system down?		√
MCDB	If data hacked from one C?	If password hacked from one C?	If one cloud down?	√	

6. CONCLUSION AND FUTURE WORK

It is clear that, although the use of cloud computing has increased rapidly, cloud computing security is a major issue in the cloud computing environment. Users do not want to lose their private information as a result of malicious insiders in the cloud. In addition, a loss of service availability has recently caused many problems for a large number of cloud users. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to propose a new model, called MCDB, which uses Shamir's secret sharing algorithm with multi-clouds instead of a single cloud. In addition, we discussed the proposed architecture with its components and layers. The aim of the proposed model is to reduce the security risks that occur in cloud computing and address the issues related to data integrity,

data intrusion, and service availability.

At this stage we compared our proposed multi-cloud model with the Amazon cloud service as a single cloud model. As a result of this comparison, it has been shown that the multi-cloud model is superior to the single cloud model in addressing the security issues in cloud computing. For future work, we plan to compare our model with other multi-cloud models and propose an improved model.

REFERENCES

- Abu-Libdeh H, Princehouse L, & Weatherspoon H (2010) RACS: a case for cloud storage diversity, Proceedings of the 1st ACM symposium on Cloud computing (ACM):229-240.
- Agrawal D, et al. (2009) Database Management as a Service: Challenges and Opportunities, Proceedings of The 2009 25th International Conference on Data Engineering (IEEE): 1709-1716.
- Akioka S, Muraoka Y (2010) HPC benchmarks on Amazon EC2, Proceedings of The 2010 24th International Conference on Advanced Information Networking and Applications Workshops (IEEE):1029-1034.
- AlZain MA, Pardede E (2011) Using Multi Shares for Ensuring Privacy in Database-as-a-Service, Proceedings of The 2011 44th Hawaii International Conference on System Sciences (HICSS) (IEEE):1-9.
- AlZain MA, Pardede E, Soh B, & Thom JA (2012) Cloud Computing Security: From Single to Multi-clouds, Proceedings of The 2012 45th Hawaii International Conference on System Science (HICSS) (IEEE):5490-99.
- Amazon (2006) Amazon Web Services. Web services licensing agreement, Accessed in May-2011.
- Amazon (2010) Amazon Web Services. Web services licensing agreement.
- Bessani A, et al. (2011) DepSky: dependable and secure storage in a cloud-of-clouds' Proceedings of the sixth conference on Computer systems (ACM):31-46.
- BNA. Privacy & security law report, 8 PVLR 10, Copyright 2009 by The Bureau of National Affairs, Inc. (800-372-1033):2009.
- Bowers KD, Juels A, & Oprea A (2009) HAIL: A high-availability and integrity layer for cloud storage, Proceedings of the 16th ACM conference on Computer and communi-

- cations security (ACM):187-98.
- Cachin C, Keidar I, & Shraer A (2009) Trusting the cloud, ACM SIGACT News 40(2):81-86.
- Cachin C, Haas R, & Vukolic M (2010) Dependable storage in the Intercloud, IBM Research 3783:1-6.
- Chockler G, et al. (2009) Reliable distributed storage, Computer 42(4):60-67.
- Clavister (2008) Security in the cloud, Clavister White Paper 1-6.
- Garfinkel SL (2007) An evaluation of amazon's grid computing services: EC2, S3, and SQS, <http://simson.net/clips/academic/2007.Harvard.S3.pdf> :1-15.
- Garfinkel SL (2003) Email-based identification and authentication: An alternative to PKI? IEEE Security and Privacy 1(6):20-26.
- Kamara S, Lauter K (2010) Cryptographic cloud storage, Financial Cryptography and Data Security, 6054:136-49.
- Kaufman LM (2009) Data security in the world of cloud computing, IEEE Security and Privacy 7(4):61-64.
- Krawczyk H, Bellare M, & Canetti R (1997) HMAC: Keyed-hashing for message authentication, in RFC Editor (ed.):1-11.
- Lee YW, et al. (2002) AIMQ: a methodology for information quality assessment, Information and Management 40(2):133-46.
- Mei H, et al. (2009) Supporting Database Applications as a Service, Proceedings of the 2009 International Conference on Data Engineering (IEEE):832-43.
- Na KS, Baik D-K, & Kim P-K (2001) A practical approach for modeling the quality of multimedia data, Proceedings of the ninth ACM international conference on Multimedia (Ottawa, Canada: ACM).
- Ristenpart T, et al. (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, Proceedings of the 16th ACM conference on Computer and communications security (ACM):199-212.
- Secombe A, Hutton A, Meisel A, Windel A, Mohammed A, & Licciardi A, et al. (2009) Security guidance for critical areas of focus in cloud computing, Cloud Security Alliance 25:1-177.
- Shamir Adi (1979) How to share a secret, Commun. ACM 22(11):612-613.
- Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications: 1-11.

Sun http://blogs.sun.com/gbrunett/entry/amazon_s3_silent_data_corruption, Accessed in May-2011.

Takabi H, Joshi JBD, & Ahn G (2010) Security and Privacy Challenges in Cloud Computing Environments, *Security and Privacy, IEEE* 8(6):24-31.

Viega J (2009) Cloud computing and the common man, *Computer* 42(8):106-08.

Vukolic M (2010) The Byzantine empire in the intercloud, *ACM SIGACT News* 41(3):105-11.

Wang C, et al. (2009) Ensuring data storage security in cloud computing, *Proceedings of The 2009 17th International Workshop on Quality of Service (IEEE)*:1-9.

AUTHOR BIOGRAPHIES



Mohammed A. AlZain is a PhD candidate in the Department of Computer Science and Computer Engineering at La Trobe University, Melbourne, Australia since Oct-2010. Currently, his PhD research is in Cloud Computing Security under Assoc/Prof. Ben Soh and Dr. Eric Pardede. He has achieved his Bachelor degree in Computer Science from King Abdulaziz University, Saudi Arabia in 2004, and then achieved his Master's degree in Information Technology from La Trobe University in 2010. He is a lecturer in the faculty of Computer Science and Information Technology at Al Taif University in Saudi Arabia. His area of interest: Cloud Computing, Database As Services.



Ben Soh is an Associate Professor in the Department of Computer Science and Computer Engineering at La Trobe University, Melbourne, Australia and a Senior Member of IEEE. He in 1995 obtained his PhD in Computer Science and Engineering at La Trobe. Since then, he has had numerous successful PhD graduates and published more than 150 peer-reviewed research papers. He has made significant contributions in various research areas, including fault-tolerant and secure computing, and web services.



Eric Pardede received the Master of Information Technology degree and Ph.D. degree in computer science from La Trobe University, Melbourne, Australia, in 2002 and 2006, respectively. He is currently a Lecturer with the Department of Computer Science and Computer Engineering, La Trobe University. He has wide range of teaching and research experience including in the area of databases, software engineering, information systems, entrepreneurship, and professional communication.