

Multi-Cloud Database Model (MCDB) to Ensure Security in Cloud Computing

Natya Achappa U
8th Sem, Computer Science & Engineering
Department
Coorg Institute of Technology
Ponnampet, South Kodagu
natya.achappa@gmail.com

Navile Nageshwara Naveen
Lecturer, Computer Science & Engineering
Department
Coorg Institute of Technology
Ponnampet, South Kodagu
nnnaveen.nag@gmail.com

Abstract— Security is considered to be one of the most critical aspects in a cloud computing environment due to the sensitive and important information stored in the cloud for users. Users are wondering about attacks on the integrity and the availability of their data in the cloud from malicious insiders and outsiders, and from any collateral damage of cloud services. These issues are extremely significant but there is still much room for security research in cloud computing.

This paper focuses more on the issues related to the data security and privacy aspects in cloud computing, such as data integrity, data intrusion, service availability. It proposes a Multi-clouds Database Model (MCDB) which is based on Multi-clouds service providers instead of using single cloud service provider such as in Amazon cloud service. In addition, it will discuss and present the architecture of the proposed MCDB model and describe its components and layers. The results and implementation for the new proposed model will be analyzed, in relation to addressing the security factors in cloud computing, such as data integrity, data intrusion, and service availability.

I. INTRODUCTION:

The need for Data outsourcing or database as a service (DaaS) is extremely important for any organization. In addition, data storage or data retrieval cost high especially for small companies [17]. Economic computing resources and advanced network technology is referred to as cloud computing [19]. The use of cloud computing has increased rapidly in many organizations. The fast access to applications or the decreasing of the infrastructure costs are provided by cloud computing services [27].

The security of Cloud computing is considered to be the most critical issue in cloud computing environment due to the valuable stored information

for users in the cloud. Cloud providers should address privacy and security issues as a matter of high and urgent priority [8]. As a result of the importance of data security in cloud computing, this paper focus more on the issues related to the data security aspect of cloud computing. It proposes a Multi-clouds Database Model (MCDB) which uses Multi-clouds service providers instead of using single cloud service provider such as in Amazon cloud service [5]. The purpose of the proposed new model is to address the security and the privacy risks challenges in cloud computing environment. There are three security factors that will be examined in our proposed model, namely data integrity, data intrusion, and service availability.

The remainder of this paper is organized as follows. Section II discusses an example of single cloud service providers which is Amazon cloud service. In addition, it mentions about Shamir's secret sharing algorithm which used in our newly proposed model. Section III describes the security risks in cloud computing with the advice of moving towards multi-clouds. Section IV proposes a new model called MCDB, with a thorough data flow explanation. Section V discusses the analysis and implementation for the new proposed model. Section VI concludes the paper with the suggestion of future work.

II. RELATED WORK

This section presents an example of single cloud to compare it with our proposed model. In addition, it mentions about Shamir's secret sharing algorithm which have been used in our proposed model.

A. Cloud Computing

Researchers in [9], [18], [26], [30] define cloud computing as “a style of computing where massively scalable IT-enabled capabilities are delivered ‘as a

service' to external customers using Internet technologies''. Cloud computing consist of three components such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Amazon web service [19] is an example of IaaS, GoogleApps is an example of PaaS and the Salesforce.com CRM application [27],[29] is an example of SaaS.

B. Single Cloud Provider

One of the first cloud computing implementations to deliver project services through a website was introduced by Salesforce.com in 1999 [3]. Amazon Web Services in 2002 provided customers with advantages such as storage and computation services. In 2006, Amazon provided their customers with the Elastic Compute Cloud (EC2) service to allow them to use their instance for data processing and computing [20]. Amazon produced the Amazon Elastic compute Cloud (EC2) as a cloud service [5] to allow users to purchase computational resources, without the need to have significant technical background to deal with the cloud computing environment. Users can focus on their own application instead of maintaining the cloud environment software and hardware. Amazon EC2 is a virtual machine that provides users with a super computer equivalent without the need to purchase it. The cost of renting the services of a cloud service provider (as-you-go) is cheaper than purchasing a super computer for the same purpose [3]. Because of Amazon EC2 instances are virtual machines, so they do not have the ability to backup the changes on disks, hence the changes on the virtual disk are lost when the instance is shut down. Therefore, in order to save modifications, the user should save them in Amazon Simple Storage Service (S3) [3]. Public cloud services for data storage, such as S3 in Amazon, provide customers with dynamic and scalable storage services. The public cloud protects the user from the cost of purchasing hardware and software for their storage infrastructure; instead, they pay a cloud service provider.

C. Shamir's Algorithm

In previous research [4] 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 (multiservice providers [2]) and also it is based on Shamir's secret sharing algorithm [25]. Our previous research gives more details about Shamir's algorithm [4].

III. CLOUD COMPUTING SECURITY

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

A. 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 [31]. Users who use online data sharing or network facilities are aware of the potential loss of privacy [12]. According to a recent IDC survey [14], the top challenge for 74% of IT executives on CIO's of cloud computing adoption is related to security matters. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance [22]. Moving databases to a large data centre involves many security challenges [33] 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 [27] present some 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 [24], their EC2 addressed security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data. Ristenpart et al. [23] claim that the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact in the private cloud.

As the cloud services have been built over the internet, any issue that is related to internet security will also affect the cloud services. Resources in the cloud are accessed through the internet; consequently even if the cloud provider focuses on security in the cloud infrastructures, the data is still transmitted to the users through the internet network which may be insecure. As a result, the impact of internet security problems will affect the cloud. Moreover, cloud risks are more dangerous due to valuable resources stored within them and cloud vulnerability. The technology used in the cloud is similar to technology used in 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 [27].

B. Why Moving to Multi-Clouds

The migration of cloud computing from single toward multi-clouds to ensure the security of user's data is extremely important. The term "multi-clouds" is similar to the terms "intercloud" or "cloud-of-clouds" that were introduced by Vukolic [32]. They also suggest 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 [1], [7], [10], [11], which control several clouds and avoids dependency on any one individual cloud. Moving from single cloud or inner-cloud to multi-clouds is reasonable and important for many reasons. According to Cachin et al. [12] "Services of single cloud are still subject to outage". In addition, Bowers et al. [10] showed that over 80% of company management "fear security threats and loss of control of data and systems". Vukolic [32] assumes that the main purpose of moving to intercloud is to improve what was offered in single cloud by distributing the reliability, trust, and the security among multiple cloud providers. Furthermore, reliable distributed storage [13] which utilizes a subset of Byzantine fault tolerance (BFT) techniques has been suggested by Vukolic [32] to be used in multi-clouds. A number of recent studies in this area have built protocols for intercloud [1], [7], [10], [11].

IV. PROPOSED MODEL

In this section, we propose a new model called Multi-clouds Database (MCDB). MCDB ensures security and privacy in cloud computing environment and is based on multi-clouds service providers and the secret sharing algorithm. These techniques have been used in previous database security research [4]. MCDB provides "cloud database" which permit customers with different types of database queries such as aggregation and exact match and range query with the ability to store any different types of data such as video, pictures or documents. The purpose of the proposed new model is to avoid the risk of malicious insider in the cloud and to avoid the failing of cloud services. The security risks such as, data integrity, data intrusion, and service availability will be examined in the model.

A. Multi-Clouds Database Model

Figure 1 illustrates the general overview of cloud computing environment. Part A represents the client

side, which sends data inquiries to server or instance such as in Amazon in cloud service provider (CSP) in part B. The data source in part B stores the data in the cloud side which is supposed to be a trusted cloud, additional to ensuring the privacy of any query that the client has made and for the security of the client stored data. A problem occurs when we cannot guarantee cloud is a trusted service

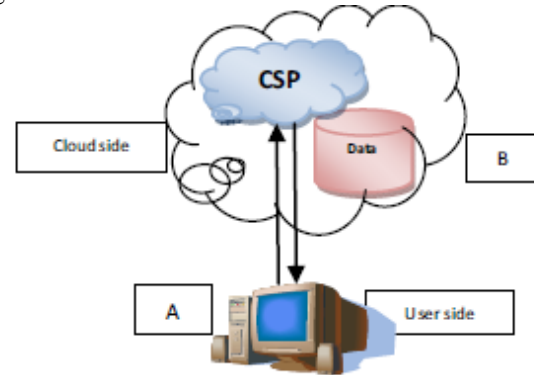


Figure 1. General overview of user/cloud Model.

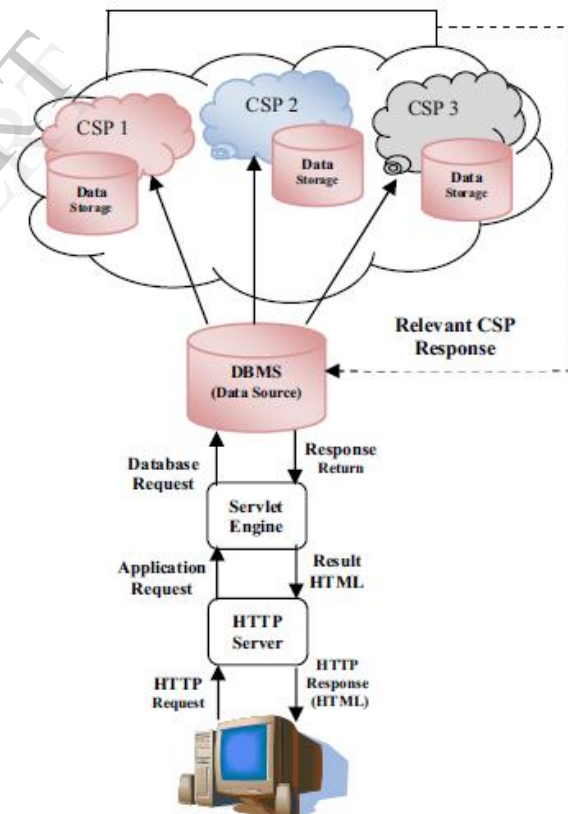


Figure 2. General Overview of Multi-clouds.

MCDB provides cloud with database storage in multi-clouds service provider which is different than Amazon cloud service. MCDB model (see Figure 2) does not preserve security by single cloud; rather

security and privacy of data will be preserved by applying multi shares technique [4] on multi-cloud providers. By doing so, it avoids the negative effects of single cloud, reduces the security risks from malicious insider in cloud computing environment, and reduces the negative impact of encryption techniques.

MCDB preserves security and privacy of user's data by replicating data among several clouds and by using the secret sharing approach. It deals with the database management system DBMS (data source) to manage and control the operations between the clients and the cloud service providers (CSP). Table 1 describes each component in the proposed model. Dividing data depend on the number of CSP to store it is considered the main factor in the secret sharing approach.

B. 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.

C. The MCDB Model Data Flow

This section will discuss the data flow for the MCDB model and shows the procedure of sending the data to the DBMS and how the users can run queries through the model in secure and private way. In addition, it describes how DBMS manages the data and divides them into shares and distributes shares into separate instances in different CSP.

- **Sending Data Procedure.** As can be clearly seen in Figure 2, 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. After that, 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 CSP. 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.

- **Procedure between DBMS and CSP.** In this section, we describe the data flow from DBMS to the multi-cloud providers in our proposed model MCDB. DBMS divides the data into n shares and stores each share in a different CSP (see Figure 3). After that, the DBMS generates a random polynomials function in the same degree for each value of the valuable attribute that the client wants to hide from the un-trusted 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 CSP) at the data source. When a user's query arrives at the DBMS, the DBMS rewrites n queries one for each CSP and the relevant share will be retrieved from CSP. For example, the rewritten query for CSP1 retrieves all workers whose salary is $share(2000,1)$ where the secret value is the salary 2000 and the cloud service provider is CSP1. 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 $p_{2000}(xi)$. After retrieving the relevant tuple from CSP, D computes the secret value to send to the client through the secured and private network. The secret sharing method can be applied to execute different types of query such as exact match, range, and aggregation query.


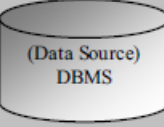

Component	Description
	End user's web browser is responsible for displaying user interface.
HTTP Server	HTTP server is responsible for managing the communication between the application and the browser. The user interface is generated by the execution from the application for server side logic.
Servlet Engine	The Servlet Engine communicates with the data source through the JDBC protocol.
	DBMS is responsible for rewriting the user's query (one for each CSP), 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 CSP and then receiving the result from CSP.
	CSP 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.

Table 1: Description for MCDB Components.




Layer Name	Component
Presentation Layer	 HTTP Server
Application Layer	Servlet Engine
Management Layer	 DBMS (Data Source)  CSP

Table 2: MCDB Layer.

V. ANALYSIS AND IMPLEMENTATION

This section discusses three issues. Firstly, it describes MCDB scenario and how the working of its components will be. Secondly, it analyzes and compares between the MCDB model and Amazon cloud service model in terms of data integrity, data intrusion, and service availability. Thirdly, it outlines the experimentation of the new proposed model. The goal of this experiment is to examine the effectiveness of the MCDB model and to simulate its operations for storing and retrieving data procedure.

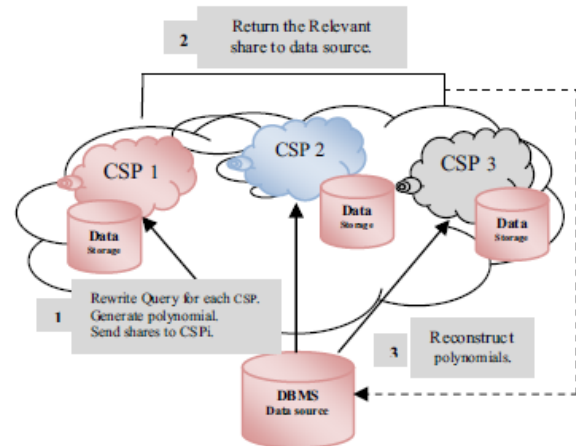


Figure 3. Procedure between DBMS/CSP.

A. MCDB Scenario

In our proposed model, DBMS divides the data that the user wants to hide from the un-trusted Cloud provider into n shares or clusters. After dividing the data (assuming the data is a numeric value, for example, worker's salary) into 3 shares and storing them in different CSPs, the DBMS generates random polynomial functions with 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 CSP. For this scenario, the value of $n = 3$ and $k = 2$. 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 CSP1 and stored as 1100 at CSP2 and stored as 1200 at CSP3. At this stage, the user's query should have arrived at the DBMS and DBMS should rewrite the query again to retrieve the result from the relevant share from CSP. Then, DBMS computes the secret value to send it to the client. 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 to apply a converted attribute to the schema. In other words, any word consists of 27 possible characters which are enumerated ($=0, A=1, B=2, C=3, \dots, Z=26$). 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 (185195182215918) and will execute the polynomial functions on this value before it is stored in CSPs.

B. What Makes MCDB Different?

Our proposed MCDB model differs from Amazon cloud service in the following three security factors:

- **Data Integrity.** One of the most important issues related to cloud security risks is data integrity. The stored data in the cloud storage may suffer from any damage occur during transition operations from or to the cloud storage provider. The risk of attacks from both inside and outside the cloud provider exists and should be considered. For example the data integrity has been recently compromised in Amazon S3 where users suffered from data corruption [28]. Garfinkel [16] argues that information privacy is not guaranteed in Amazon S3. Data authentication assures that the returned data is the same stored data 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 [21] technology or a digital signature to ensure data is not modified by Amazon S3. These technologies protect users from Amazon data modification and from hackers if they have stolen their email or password [16].

However, as explained before, the proposed MCDB model used multi-clouds which is different from the Amazon cloud service. In addition, the use of Shamir's secret approach makes MCDB different. For example, the data will be distributed into three different cloud providers in MCDB model. In addition, the secret sharing algorithm will be applied on the stored data in the multiple cloud providers. If the intruder or malicious insider wants to know the hidden information inside the cloud, they should retrieve at least three values from three different cloud service providers to be able to know the real value which has been converted and hidden before it stored at the multi clouds providers. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claim that, if there are 3 shares stored in 3 cloud providers ($n=3, k=2$), the knowledge of the value of 2 shares or less makes the secret un-constructible whereas the knowledge of the value of more than two shares will enable the value to be reconstruct. Therefore, MCDB model is superior to

Amazon cloud service in addressing the issue of data integrity.

- **Data Intrusion.** According to Garfinkel [16], another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If anyone gains access to an Amazon account password, then 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 for the user's email (Amazon user name) to be hacked (see [15] for a discussion of the potential risks of E-Mail), and 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, MCDB model is different from the Amazon cloud service. MCDB replicates the data among three different cloud providers; hackers need to retrieve all the information from the three cloud providers to be able to reconstruct the real value of the data in the cloud. In other words, if the hacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider (in our case) to know the secret which is the worst and the hardest case scenario. Hence, replicating data into multi-clouds by using a multi share technique [4] may reduce the risk of data intrusion such as in MCDB model and different than Amazon the single cloud.

- **Service Availability.** Another major concern in cloud services is service availability. Amazon [6] mentions in its licensing agreement that the unavailability of the service may occur in the Amazon Company. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon's web service and the service fails, in this case there will be no compensation from the Amazon Company regarding this failure. Companies seek to protect their services from system failure to avoid the unavailability of any related service to the

cloud providers such as backups or disconnection to any dependent cloud providers [16]. Garfinkel [16] argues that information privacy is not guaranteed in Amazon S3. Data authentication assures that the returned data is the same stored data is extremely important.

However, MCDB is different from Amazon cloud service in relation to service availability risk or loss of data. MCDB distributed the data into different cloud providers and therefore it could be argued that the data loss risk will be reduced. If one cloud provider fails, users can still access their data live in other cloud providers.

According to other research, to ensuring backup even if instances are down Garfinkel [16] advises users to run their services on multiple instances in Amazon EC2 and storing data in multiple Amazon S3, then link different Amazon Web Services (AWS) to different email's addresses. But what will happen if Amazon decided to delete user's data for any reason from their all instances depend on their web service licensing agreement (WSLA)[5]. Therefore, using multiple cloud service providers in MCDB model may reduce the risk of loss of data.

As a result of the three above arguments for data integrity, data intrusion, and service availability, our newly proposed MCDB model is better in addressing the three security factors than in Amazon cloud service and more secured in protecting user's data from untrusted cloud service providers and from the malicious insider especially when Amazon cloud service ask the users to encrypt their data before storing it in their instances, whereas, MCDB take responsibility of this task. Table 3 summarizes the differences between Amazon and our proposed MCDB model in terms of the three security factors that may occur in cloud computing environment.

	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 CSP?	If password hacked from one CSP?	If one cloud down?	✓	

Table 3: Comparison between Amazon/MCDB.

C. Implementation and evaluation

This section explains the experimentation to examine the MCDB model. The experiment is written in Java to simulate data storing in multi-cloud providers, data retrieval from different cloud providers. The experiment provides evaluation of all three types of queries, namely exact matching, range and aggregate query. For the dataset, we use numeric data. Nevertheless, we can still apply this experiment to nonnumerical data as it was explained (see section A in V).

- **Data storing procedure.** Data storing in MCDB involves data distribution from the data source to different cloud providers. This is done after executing the polynomial functions on the data. On the other hand, Amazon cloud service asks the organization to encrypt their data before store it in their instances. As comparison between Amazon and MCDB in data storing 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 for ensuring the privacy of users' queries during the data retrieval process.

To analyse the effect of a number of shares in our model, we perform experimentation for data storing in MCDB using static data size (10 MB). Figure 4 shows that the time cost for the data storing 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 un-trusted cloud provider due to the fact that the CSPs need more numbers 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.

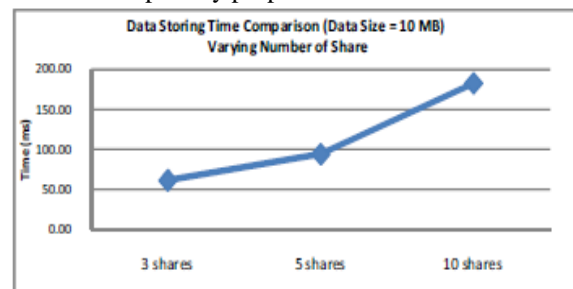


Figure 4. Data Storing Time Comparison, Varying Shares.

Data retrieval procedure. For data retrieval, we simulate different types of queries such as the exact match, aggregation and range query in MCDB model which is not provided by Amazon cloud service. These different types of queries what differentiate

MCDB model from Amazon cloud service. The data retrieval process in the MCDB model starts from rewriting the user's query in the DBMS (n numbers of queries) and then sends these queries, one for each CSP, 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 example for intra-comparison to evaluate the different types of queries inside our MCDB model, we run our experiment to compare between exact match and aggregation query in our model and we found that the exact match query outperform the aggregation query as it is clear in Figure 5.

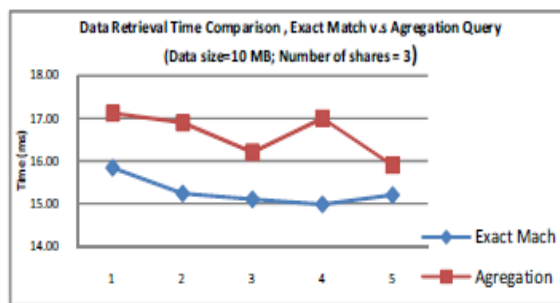


Figure 5. Data retrieval time Comparison, Varying queries.

As an evaluation for the outcomes of data retrieval for various numbers of shares in the secret sharing algorithm in MCDB model, Figure 6 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 CSPs will need to retrieve more values from more shares in order to be able to determine the hidden information in CSPs.

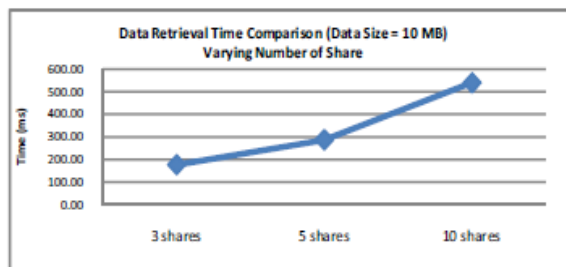


Figure 6. Data Retrieval Time Comparison, Varying Shares.

VI. CONCLUSION AND FUTURE WORK

It is clear that although the use of cloud computing

has increased rapidly, cloud computing security is considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. 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 use Shamir's secret sharing algorithm with multi-clouds providers instead of single cloud. In addition, it is discussed its architecture with its components and layers. The aim of this model is to reduce the security risks occurs in cloud computing and addresses the issues that related to data integrity, data intrusion, and service availability.

At this stage we compared our proposed multiclouds model with Amazon cloud service as a single cloud model. As a result of this comparison, it has shown that the multi-clouds model is superior than single cloud model in addressing the security issues in cloud computing. For future work we plan to compare our model with other multi-clouds models or systems to go further in our comparison until we get the best and improved model.

REFERENCES

- [1] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, *RACS: a case for cloud storage diversity*, ACM, 2010, pp. 229-240.
- [2] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, *Database Management as a Service: Challenges and Opportunities*, *Data Engineering, 2009. ICDE '09. IEEE 25th International Conference on*, 2009, pp. 1709-1716.
- [3] S. Akioka and Y. Muraoka, *HPC benchmarks on Amazon EC2*, IEEE, 2010, pp. 1029-1034.
- [4] M. A. AlZain and E. Pardede, *Using Multi Shares for Ensuring Privacy in Database-as-a-Service*, *2011 44th Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1-9.
- [5] Amazon, *Amazon Web Services. Web services licensing agreement*, (2010).
- [6] Amazon, *Amazon Web Services. Web services licensing agreement, October 3, 2006*, (2006).
- [7] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, *DepSky: dependable and secure storage in a cloud-of-clouds*, ACM, 2011, pp. 31-46.
- [8] P. BNA. Privacy & security law report, 03/09/2009. Copyright 2009 by The Bureau of National Affairs, Inc. (800-372-1033), 2009
- [9] M. P. Boss G, Quan D, Legregni L, Hall H. , *Cloud computing*, (2009), p. 4.
- [10] K. D. Bowers, A. Juels and A. Oprea, *HAIL: A high-availability and integrity layer for cloud storage*, ACM, 2009, pp. 187-198.
- [11] C. Cachin, R. Haas and M. Vukolic, *Dependable storage in the Intercloud*, Research Report RZ, 3783 (2010), pp. 1-6.

- [12] C. Cachin, I. Keidar and A. Shraer, *Trusting the cloud*, ACM SIGACT News, 40 (2009), pp. 81-86.
- [13] G. Chockler, R. Guerraoui, I. Keidar and M.Vukolic, *Reliable distributed storage*, Computer, 42 (2009), pp. 60-67.
- [14] Clavister, *Security in the cloud*, Clavister White Paper (2008), pp. 1-6.
- [15] S. L. Garfinkel, *Email-based identification and authentication: An alternative to PKI?*, IEEE Security and Privacy (2003), pp. 20-26.
- [16] S. L. Garfinkel, *An evaluation of amazon's grid computing services: EC2, S3, and SQS*, Citeseer, 2007, pp. 1-15.
- [17] B. I. H. Hacig, C. Li and S. Mehrotra, *Executing SQL over encrypted data in the database-serviceprovider model*, Proceedings of the 2002 ACM SIGMOD international conference on Management of data, ACM, Madison, Wisconsin, 2002, pp. 216-227.
- [18] J. Heiser, *What you need to know about cloud computing security and compliance*, Gartner, Research, ID (2009).
- [19] S. Kamara and K. Lauter, *Cryptographic cloud storage*, Financial Cryptography and Data Security (2010), pp. 136-149.
- [20] L. M. Kaufman, *Data security in the world of cloud computing*, IEEE Security & Privacy (2009), pp. 61-64.
- [21] H. Krawczyk, M. Bellare and R. Canetti, *HMAC: Keyed-hashing for message authentication*, Citeseer, 1997, pp. 1-11.
- [22] H. Mei, J. Dawei, L. Guoliang and Z. Yuan, *Supporting Database Applications as a Service*, Data Engineering, 2009. ICDE '09. IEEE 25th International Conference on, 2009, pp. 832-843.
- [23] T. Ristenpart, E. Tromer, H. Shacham and S. Savage, *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*, ACM, 2009, pp. 199-212.
- [24] H. A. Seccombe A, Meisel A, Windel A, Mohammed A , Licciardi A, etal., *Security guidance for critical areas of focus in cloud computing*, CloudSecurityAlliance, 2009, p. 25. (2009).
- [25] A. Shamir, *How to share a secret*, Commun. ACM, 22 (1979), pp. 612-613.
- [26] R. Stanojevi and R. Shorten, *Fully decentralized emulation of best-effort and processor sharing queues*, ACM, 2008, pp. 383-394.
- [27] S. Subashini and V. Kavitha, *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications (2011), pp. 1-11.
- [28] Sun, [//blogs.sun.com/gbrunett/entry/amazon_s3_silent_data_corruption](http://blogs.sun.com/gbrunett/entry/amazon_s3_silent_data_corruption).
- [29] H. Takabi, J. B. D. Joshi and G. Ahn, *Security and Privacy Challenges in Cloud Computing Environments*, Security & Privacy, IEEE, 8 (2010), pp. 24-31.
- [30] L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, *A break in the clouds: towards a cloud definition*, ACM SIGCOMM Computer Communication Review, 39 (2008), pp. 50-55.
- [31] J. Viega, *Cloud computing and the common man*, Computer, 42 (2009), pp. 106-108.
- [32] M. Vukolic *The Byzantine empire in the intercloud*, ACM SIGACT News, 41 (2010), pp. 105-111.
- [33] C. Wang, Q. Wang, K. Ren and W. Lou, *Ensuring data storage security in cloud computing*, IEEE, 2009, pp. 1-9.