# Data mobility management model for active data cubes

Thanh Dat Dang
Centre for Innovation in IT Services
and Applications (iNEXT)
University of Technology Sydney,
Australia
ThanhDat.Dang@uts.edu.au

Doan Hoang
Centre for Innovation in IT Services
and Applications (iNEXT)
University of Technology Sydney,
Australia
Doan.Hoang@uts.edu.au

Priyadarsi Nanda
Centre for Innovation in IT Services
and Applications (iNEXT)
University of Technology Sydney,
Austraslia
Priyadarsi.Nanda@uts.edu.au

***Abstract*—Cloud computing dramatically reduces the expense and complexity of managing IT systems. Business customers do not need to invest in their own costly IT infrastructure, but can delegate and deploy their services effectively to cloud vendors and service providers. A number of security and protection mechanisms have been proposed to prevent the disclosure of sensitive information or tempering with the data by employing various policy, encryption, and monitoring approaches. However, few efforts have been focused on data mobility issues in terms of protection of data when it is moved within a cloud or to and from a new cloud environment. To allay users' concern of data control, data ownership, security and privacy, we propose a novel data mobility management model which ensures continuity protecting data at new cloud hosts at new data locations. The model provides a mobility service to handle data moving operation that relies on a new location database service. The new model allows the establishment of a proxy supervisor in the new environment and the ability of the active data to record its own location. The experimental outcomes demonstrate the feasibility, proactivity, and efficiency by the full mobility management model.**

***Keywords*—data mobility, data protection, cloud mobility, data location**

## I. Introduction

Cloud computing has been gaining acceptance across various domains ranging from business to research [1]. In order to make effectively use of cloud services, users' data is stored in a cloud where applications are able to perform more cost-effectively requests from clients. Two major concerns arise naturally: first, users are concerned that they lose the control of their data once it is transferred to the cloud, and second, cloud service providers are concerned that they may not be able to protect the data effectively when it is moved about both within and out of its own cloud environment. Despite the fact that cloud service providers have provided security mechanisms to deal with this issue by employing various policy and encryption approaches. While data is particularly protected at its home cloud, it still exposes to potential disclosure and attacks if located at another cloud where there is no equivalence security measure at different sites from different CSPs [2]. Consequently, these data mobility issues have to be addressed in any data security models for cloud. Despite of the issues associated with interoperability and exchange information issues among cloud, user's data should still be protected at new cloud environments with compatible or equivalent measures it enjoys in its home environment.

In a realistic cloud scenario with complex and dynamic hierarchical service chain, the handling of data in a cloud can be delegated to another. However, CSPs do not often deploy the same protection schemes [2]. In addition, when user's data is moved to data centers located at locations different from its home, it ought to register with a supporting service to report its locations to the original cloud and its data owner. This may be achieved if these CSPs have agreed on a Service Level Agreement (SLA) that enables establishing a required monitoring service from the original cloud. When a violation against the established SLA occurs, the monitoring component will be able to detect it through the corresponding CSP and trigger protection services on the original cloud which can immediately analyse and audit the data. Moreover, data locations need to be maintained at the original cloud and encoded within the data itself in case it loses the connection with its monitoring service. Under such circumstances, the location data can be used subsequently to trace previous locations and data operations or trigger original mobility services if data is moved back to a Cloud. For the users, they are concerned whether their data is located in locations covered by the SLA and data operations are protected from unauthorised users. Mechanisms should be available to report information concerning the data, such as the data location, access, or violation, to their owner if and when necessary.

This paper addresses the above concerns from a novel perspective, offering a data mobility management model with enhanced transparency and security. In this model, we extend our active data framework with an appropriate data structure and a Location Registration Database (LRD) to deal with mobility; we investigate protocols between clouds for data movement; we investigate procedures for establishing a clone supervisor at a visited cloud for monitoring purposes. The proposed data mobility model focuses on two aspects: data mobility management (DMM) and active protection service. The DMM deals with physical location changes of user's data in various cloud environments, and ensures these locations be recorded at LRD as well as within the data itself and whether the new physical location conforms to the pre-established

SLA. The active protection service deals with extending data protection when the data is moved to various locations.

The rest of the paper is organized as follows. Section II discusses related work on data mobility in cloud. Section III reviews briefly our Trusted-Oriented Data Protection Framework proposed in an earlier work. Section IV defines components and parties involving in the mobility model and introduces data moving cases. Section V presents the design of the proposed data mobility management model. Section VI presents an implementation for the model. Section VII present the evaluation and analysis of the proposed model. The conclusion and future work will be drawn in the section VIII.

## II. RELATED WORK

Ries et al. [3] focused on verifying geographic data location in a cloud environment, detecting data movements and proving data possession for data moving among CSPs. However, these efforts mainly relied on network latency and distance between Clouds and focused little on data protection and relationship between data and users.

Chen and Hoang [4] proposed an active data binding framework in addressing data mobility and user mobility. This research concentrated on notifying data owners when their data is moved from one location to another, tracking data geographic location using Google services and integrating active data-centric framework to collect evidences of data movement. However, the lack of secured components or equivalence protection schemes at the new location results in data violation and illegal disclosure as there in no monitoring services to track the data and prevent illegal requests. Consequently, data cannot be independently survived in the heterogeneous cloud environment.

Popa [5] proposed a data traceability service for mobile computing application. A security framework for this service includes security components which ensure integrity, authenticity, confidentiality and non-repudiation and management components which apply the appropriate security components to user's private data. Users can create a request to read, modify or even transfer the data via mobile applications. When a request is performed, a message from a trace service will notify the user that his private data was accessed. This approach only considers the case that the data is accessed by data owner. There is no data movement from one Cloud to another. A request to send data is simply performed by creating a copy of the data. The data sent by user will not be traced by the service.

Betge-Brezetz [6] proposed a privacy control model at the Virtual Machines (VM) level to protect sensitive files stored, processed, and moved in an Infrastructure as a Service (IaaS) cloud. The demonstration involved clouds located in different countries and but run on the same platform. The model requires cloud service providers to build the same cloud platform and establish the same privacy control modules in order to protect the data moving among clouds. Overhead is an issue at this VM control level.

Nikolay Tcholtchev [7] introduced the concept of mobility data cloud in which a cloud is utilized as a platform for the providers. The work also proposed a framework for the acquisition, aggregation, provisioning, and analysis of mobility relevant data originating from various sources.

All the above approaches have not addressed the security requirements to protect data from violation attacks when data is located at visited cloud sites. The data mobility management model in this paper leverages our active data protection framework [8] in developing protocols for moving data among clouds and in establishing a new supervisor at a visited cloud for monitoring data and data operations at the new cloud as well as reporting the welfare of the data to the original cloud. In addition, active data will be designed with recordable structure enabling data to store various locations when data is accessed. The model enables data to be moved among clouds of different infrastructures ranging from private cloud to public cloud while ensuring data protection regardless of its location.

## III. TRUST-ORIENTED DATA PROTECTION FRAMEWORK

In an earlier work, we proposed a Trust-Oriented Data Protection Framework for data protection in Cloud environments [8].

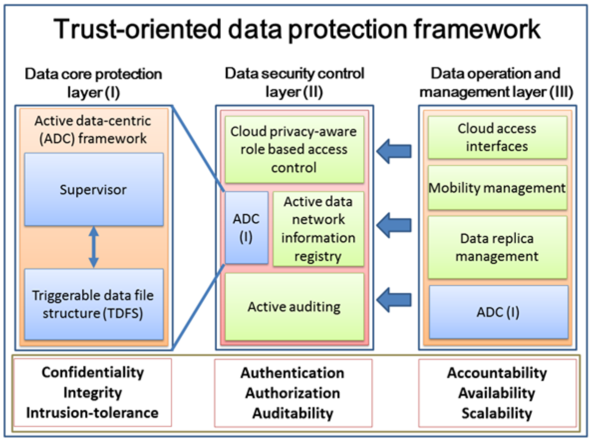

Trust-oriented data protection framework
Data core protection layer (I)
Data security control layer (II)
Data operation and management layer (III)
Active data-centric (ADC) framework
Supervisor
Triggerable data file structure (TDFS)
Cloud privacy-aware role based access control
ADC (I)
Active data network information registry
Active auditing
Cloud access interfaces
Mobility management
Data replica management
ADC (I)
Confidentiality
Integrity
Intrusion-tolerance
Authentication
Authorization
Auditability
Accountability
Availability
Scalability

Fig. 1. Trust-oriented data protection solution in cloud

Figure 1 illustrates the proposed trust-oriented cloud data protection framework. The framework is structured into 3 blocks: the data security control block provides secure access control and data auditability functions, the data core protection block provides techniques and procedures for implementing active data protection, and the data operation and management block handles mobility and data replication management. This framework can be considered as a secure data container that manipulates, and verifies the data within without the involvement of a third party service. This structure presents a security and trust abstraction at a higher level than conventional data protection models that rely on the peripheral security environment and third party protection mechanisms. Our core goal is to empower data the capabilities of self-defend and self-protect against intrusions or violations. Data misbehaviour and violation can be actively detected by the data itself, reducing the risk of use by adversaries. The data core protection block employs an active security approach whereby the data is made active against any invocation, whereas the data security control block and data operation and management block support this active approach by providing data auditing and other measures including secure access control, data replication and mobility.

A unit of raw data is transformed into a novel data structure called a Triggerable Data File Structure (TDFS). The TDFS consists of a shell and a core as shown in Figure 2. The shell is equipped with active tamper-proofing codes and is executed prior to the core when the TDFS is triggered. A TDFS is also referred to as an Active Data Cube (ADCu). The core of the TDFS comprises an executable segment, a header, and data blocks. The runnable scripts in the executable segment allow basic data operations, data loading, and data analysis functions. The header refers to a manifest specifying the basic information related to the data such as security header, data descriptor, and timestamp. Raw data blocks are encrypted.

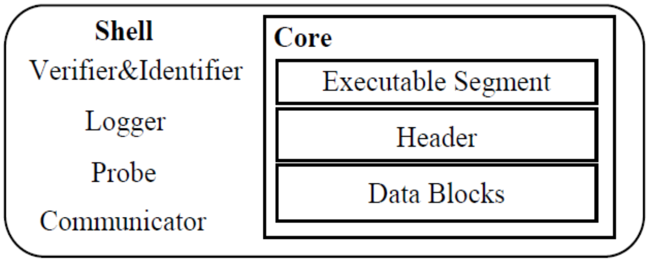


Fig. 2. Structure of an Active Data Cube

As the ADCu can only protect and manage the contents within, it cannot be triggered if adversaries attempt to execute operations such as move or delete the whole data cube. The supervisor thus is designed to monitor operational system (OS) level data manipulations that cannot be detected by the ADCu itself. An atomic data security model, called the Active Data Protection unit (ADPu), is needed for supporting the active protection functions of the ADCu within the protection framework. The APDu is an atomic component combining two entities: a supervisor and an ADCu.

The management and coordination of Cloud data for each tenant is processed by the supervisor, an active service instance that is activated when the corresponding tenant subscribes to cloud storage services.

In this framework, two services are proposed for data security control: the Cloud Privacy-aware Role Based Access Control (CPRBAC) service and the Active Auditing Control (AAC) service. The CPRBAC service defines and describes the security boundary on data operations in cloud. Resource requests that are not allowed in the policy repository will be rejected. The AAC is introduced to execute and audit users' requests in a secure and consistent manner. Users' requests must be actively audited under a distributed transaction management session.

## IV. COMPONENTS OF THE DATA MOBILITY MODEL AND DATA MOVING CASES

Even with the Trusted-Oriented Data Protection Framework, the data is still exposed to potential violations when it is moved to new cloud hosts where there are no equivalence security measures to protect it. Data mobility is still a challenge for exchanging information among CSPs due the lack of approaches to ensure data protection and data auditing. Our earlier work only explored a simple mechanism for data-binding mechanism that allows the active data to alert its owner when it is moved to a new environment.

Clearly, mobility management is one of the most important challenges in mobile IP [9]. When a mobile is roaming away from its home network, it registers its current location to its home agent on home network. Similarly, when a data unit moves from its original cloud, it needs to inform the original cloud its current locations and may also inform data owner its status. The data itself, however, cannot execute these actions. In this paper, we leverage the ideas from mobile network about location register for a mobile by investigating a new LRD located at original cloud to serve for updating or retrieving data locations and a new recordable data structure enabling to record cloud host location in the data when there is any request data operations. Moving data to a new cloud environment, however, has to involve both the data and its supervisor. In our model we propose a scheme for establishing a clone supervisor for monitoring the moved data and data operations. At this stage, the verification procedure will be processed data requests only at the original cloud for access permissions since the deployment of protection framework may increase the complexity. Future development of the mobility management model may delegate the verification and access control to the visited cloud. With the deployment of the supervisor, data protection can be achieved despite the fact that data is located at visited cloud side.

### *A. Parties and Components in a data mobility management model*

We define functions of parties involving in the mobility management model as follows.

1) **An old cloud** can be an original cloud or a visited cloud offering cloud resources from clients. While an original cloud can offer cloud resources and verification procedure, a visited cloud is simply storing, providing data and forwarding verification requests for permission. A request from a new cloud or within an existing cloud for accessing cloud resources or to verify users' permission will be submitted to the cloud interface. Since this request has to obtain an access right to use the data, the old cloud will define a common user interface for both kinds of request including parameters such as Source address, Destination address, Data_ID, Operation, TimeStamp. Then it will be forwarded to the CPRBAC service at the original cloud for verification. Only verified requests can be forwarded to the supervisor which will command the movement of its TDFS and invokes the mobility service for updating new data location.

2) **A new cloud** creates a request to access cloud resources with appropriate parameters. The old cloud and the new cloud

will have to agree in launching a clone supervisor at the new cloud to monitoring, protecting the moved data against any violation. In addition, the request has to specify its access purposes in order to meet obligations to the original cloud. As a result, the original cloud is able to process the request by approving resources or triggering protection services to lock requests and send an alarm to specific data owner or administrator.

3) **A supervisor** is responsible for protecting its associated data, data locations and communication among clouds. It is created to monitor and detect data operations in cloud. To allow data mobility, a clone supervisor will be established at the new cloud based on agreements between the two clouds. Main functions of a supervisor include data verification and data location management.

- Data verification: the supervisor monitors data operations either at the original cloud or the visited cloud. Data only accepts instructions from its supervisor. For monitoring function, the supervisor focuses mainly on detecting user's operations at the operation system OS level such as move, copy and delete. When the supervisor detects such a request, it would activate the TDFS through instructions to execute the runtime environment analysis and inspect the validity of data operations. In our active data model, data operations will be verified at the shell which wraps the data in an executable status.

- Data location management: the supervisor also reports timely data locations to the original cloud as well as updating the LRD since data itself cannot send location information to original cloud but it is able to record current location for tracing operations. It analyses networking location in order to obtain the current network address and send back to original cloud which is set as default source address in the report message.

### *B. Establishing new supervisor procedure*

It is assumed that the new cloud and the original cloud agree to establish a new supervisor at the new site. Since the verification is processed at the original side, the new clone supervisor is for dealing with data moving cases among clouds. In the first case, data is moved from an original cloud to a new cloud (the request may be originated from the original cloud or from the new cloud). In the second case, data at an old cloud is moved to a new cloud and original cloud will process request verifications. In the third case, data at an old cloud is moved back to the original cloud; and in the last case, data at a cloud is moved to local storage (offline) with or without permissions.

In the first case, when the original cloud receives a request to move data to the new cloud, it will verify and analyse the request to obtain the destination address. There are two possible scenarios: the request comes from the new cloud and the request comes from an entity in the home cloud such as the data owner or the administrator. In both scenarios, a general procedure has to be executed between the two clouds before moving the data. The procedure is as follows:

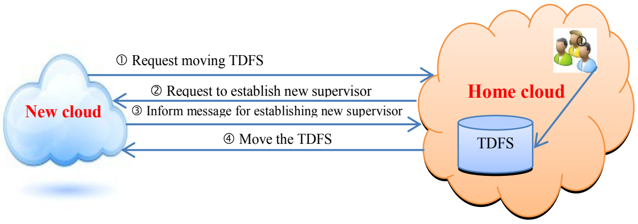

① Request moving TDFS
② Request to establish new supervisor
③ Inform message for establishing new supervisor
④ Move the TDFS
New cloud
Home cloud
TDFS

Fig. 3. General establishing supervisor procedure

1. After analysing the request, the original cloud sends a request to the new cloud for establishing a new supervisor at the new cloud. This effectively requests the visited cloud for the permission to install a new service. At this time, the new cloud also verifies the request to evaluate wherever it can or cannot create the service. If there is the agreement between two clouds to create the new supervisor, a confirmed message will be sent from the new cloud to the home cloud.
2. Following the first step, information pertaining to the supervisor and the TDFS including the type of services, of the template of the supervisor, and the original location will be sent to the new cloud for creating a new instance of the supervisor.
3. After the supervisor is created, the TDFS will be moved to new cloud.

The new supervisor will be responsible for monitoring the TDFS at the new cloud as well as communicating with the original cloud since the new cloud does not provide the same data protection services.

If the request originated from an entity in the home cloud, the destination address of the new cloud where data is to be moved to, has to be provided with the request. Once the destination address is identified, the home cloud can communicate with the new cloud. In both scenarios, security procedures are performed by the access control component, the CPRBAC, and the auditing component, the AAC together with the associated supervisor. Having satisfied with the conditions for moving the requested data, the home cloud sends a request in order to establish the clone supervisor at the new cloud. By doing this, the link between the supervisor and its data is still kept when data is stored at another location. Details of the procedure as follows.

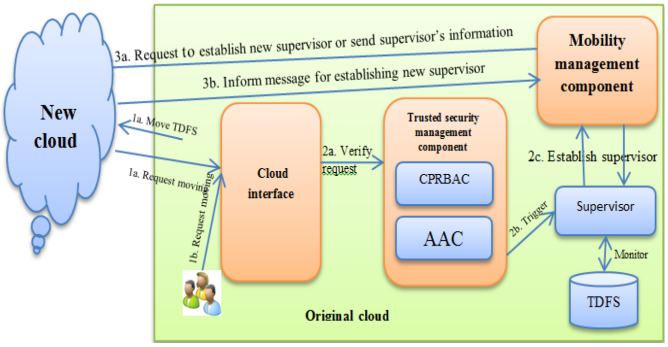

New cloud
3a. Request to establish new supervisor or send supervisor's information
3b. Inform message for establishing new supervisor
Mobility management component
1a. Move TDFS
1a. Request moving
1b. Request moving
Cloud interface
2a. Verify request
Trusted security management component
CPRBAC
AAC
2b. Trigger
2c. Establish supervisor
Supervisor
Monitor
TDFS
Original cloud

Fig. 4. Details of establishing supervisor procedure

1. The service request from the new cloud or from within the original cloud is sent to the original cloud. This request is authorized by the CPRBAC and the AAC. If it is a legal request, the supervisor is triggered to analyse data operations. Since it is a “move” request, the supervisor has to communicate with mobility component for establishing a clone supervisor at the new cloud. Illegal requests against predefined policies will be triggered by the active data protection unit (APDu) and captured by the AAC. Violation triggers in the AAC may also be triggered to assist the security administrator to execute some certain security prevention operations.

2. The mobility component at the original cloud sends a request to the visited cloud for the permission to install a new service. The new cloud also verifies and evaluates the request to see if it can create the service. If an agreement is in place to create a new supervisor between two clouds, a confirmed message will be sent from the new cloud to the an original cloud.

3. At this step, necessary information for creating the clone supervisor will be supplied to the new cloud.

4. Once the new supervisor is created, the mobility component invokes instructions to move the data. The supervisor also queries the LRD to update the new data location.

For the second case, the procedure is similar but the verification request needs to be forwarded from the old cloud to original cloud for authorization. The third case simply moves the data back to the original cloud and update the data location in the LRD. For the last case, the regular verification procedure is still executed at the original cloud to obtain the move permission.

However, an exception will be raised when the original cloud detects a data move without a request or it cannot communicate with destination address provided in the request to establish supervisor. In these cases, the current supervisor has to report the current TDFS location to the original cloud for updating the LRD as well as triggering the data to update this address in its core component before moving. From this point, the TDFS has to record data access locations in its location list whenever users access the data even in the offline mode.

## V. MOBILITY MANAGEMENT MODEL

In this paper we focus on providing a data mobility solution for cloud data moving among clouds while ensuring data protection and auditing relevant data locations and accessed data operations. The new features of our proposed model include: an active data framework with appropriate data structure and a Location Registration Database (LRD) to deal with mobility; protocols between clouds for data movement; procedures for establishing a clone supervisor at the visited cloud for data protection purposes. In particular, there will be a mobility service agent responsible for updating and retrieving data location from the LRD. Figure 5 depicts the model and its four core components: 1) the data core protection component, 2) the mobility management component, 3) the trusted security management component, and 4) the cloud interface.

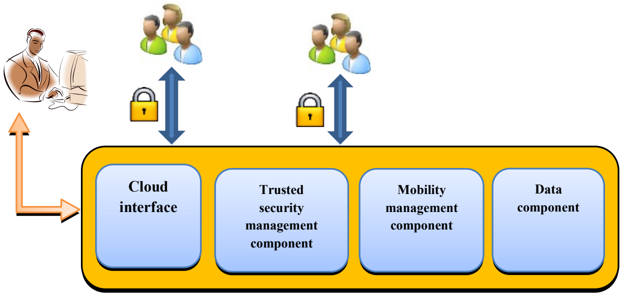

Cloud interface
Trusted security management component
Mobility management component
Data component

Fig. 5. The design of data mobility model

**1) The data core protection component:** this component is designed to enable active surveillance, smart analysis, self-protection, and self-defense capabilities directly on to the data itself. The data is transformed and encapsulated in TDFS that supports confidentiality, integrity, and intrusion-tolerance [8]. To support mobility, a special encrypted element namely Recordable Mobility Data (RMD) is designed to record user’s operations when they access the data. Only the data owner who has the decryption key can trace previous data operations. The management and coordination of cloud data for each tenant is processed by the supervisor, whose active service instance is activated when the corresponding tenant subscribes to a cloud storage service. Several supervisor service instances can be deployed to deal with a large number of requests from diverse virtual servers or machines (VMs). An atomic APDu contains an active data cube (the TDFS) and its supervisor.

**2) The mobility management component:** this component includes the Mobility Service (MS) and the LRD. It aims to store and manage information about the supervisor and the TDFS at original cloud. The component centres around the location registration procedure when TDFS is moved by maintaining connections with external supervisors.

**The MS** is responsible for creating queries to the LRD. When the data is created at a cloud, the supervisor invokes the MS to update the information about the TDFS in the LRD. In addition, MS also supports the establishment of the new supervisor at the visited cloud.

**The LRD** stores the TDFS information related to data location, data operations, and data owner for data status monitoring purposes. When a TDFS is subscribed to a cloud, it needs to register and is allocated a supervisor that is responsible for the data welfare including monitoring and raising an alarm if illegal data operations are detected. Therefore, whenever a TDFS moves out of its home cloud, the supervisor will invoke a query to extract information from the database necessary for the establishment of the clone supervisor at the new cloud.

**3) The trusted security management component:** this component is proposed to execute trusted security management. The CPRBAC service [10] is proposed to define and describe the security boundary on data operations in distributed clouds. Access resource requests that are not specified in the policy database will be rejected. The fine-grained policy structure of the CPRBAC allows users to configure and define specific and secure protection requirements on their data. Authentication and authorization will be offered by the service. The AAC [11] is introduced to execute and audit users' requests in a secure and consistent manner. Users' request must be actively audited under a distributed transaction management session. Through recording audit data created as the attestations, the CSPs can report the evidences of data violations to their users. The users are more inclined to adopt the cloud solution for their businesses as they can establish more acceptable SLA with their subscribed CSPs in a firmed trustworthy relationship. The auditability can be achieved by the AAC.

**4) Cloud interface:** Cloud access interfaces provide data service interfaces to access active data in cloud storage systems. It forwards requests with parameters to security management component to verify access permission.

## VI. Implementation

### *A. Data structure design*

**Data** is structured utilizing Active Data-Centric framework [8]. A special structure namely Recordable Mobility Data (RMD) is designed to record information associated with users' access request. The information includes Subject_ID, Data_ID, Operation, TimeStamp, and Cloud location. This information is transparent to its data owner. In other words, it is hidden from users' data operation. The stored information is encrypted using the RSA encryption to avoid possible information leakage. Only the data owner has the corresponding key to disclose them for tracing previous operations.

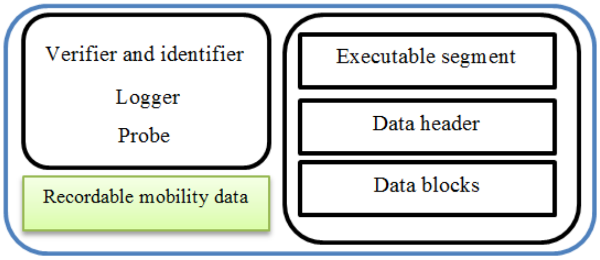


Fig. 6. Triggerable Data Structure

| Subject ID | Data ID | Data operation | Source address | Current address | Destination address | TimeStamp |
|---|---|---|---|---|---|---|

Fig. 7. Recordable mobility data structure

### *B. Data mobility management workflows*

When a customer subscribes to the cloud service, the CSP will assign roles associated with the data for users, allowing them to access a virtual user directory and workspace for the tenant, and an initial set of empty active data cubes will be created according to the regular data types. After assigning roles, the supervisor will be invoked to send a request to the mobility service for data location registration. The request containing parameter such as UserID, DataID, Location and TimeStamp will be executed as a query to update to the database. Finally, the user will receive a data location registration acknowledgement message via the mobility service. Figure 8 presents the workflow for a new data location registration.

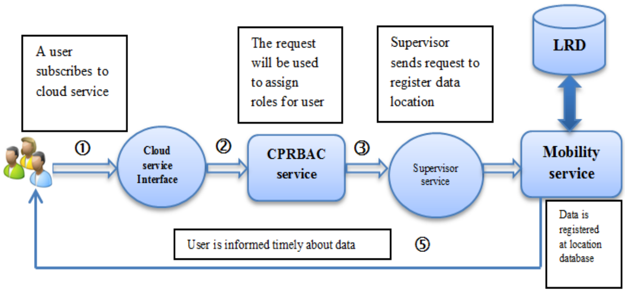

A user subscribes to cloud service
The request will be used to assign roles for user
Supervisor sends request to register data location
LRD
①
Cloud service Interface
②
CPRBAC service
③
Supervisor service
Mobility service
Data is registered at location database
User is informed timely about data
⑤

Fig. 8. New data location registration workflow

When a user needs to execute data operations such as read, insert, write and move the data, he/she will send a request to the cloud interface including a set of parameters such as UserID, DataId, Operation and Location and TimeStamp. In turn, a verification process is created to perform a sequence of steps. Firstly, it invokes the supervisor to access the data. Hence, the supervisor needs to establish the validity of the request by forward it to the original cloud where data location is also updated. If the request is not valid or allowed by the access policy, the supervisor will raise an alarm to notify the system administrator or related legislation organization. In fact, if desired, the data owner may be informed immediately when the original cloud detects the violation through the mobility service. If the request is permitted, the mobility service will update data location before approved verification is sent to the supervisor. From this point, data operations will be performed on the TDFS but each operation is recorded inside the TDFS for tracing purposes. Figure 9 presents the general procedure for data mobility workflow

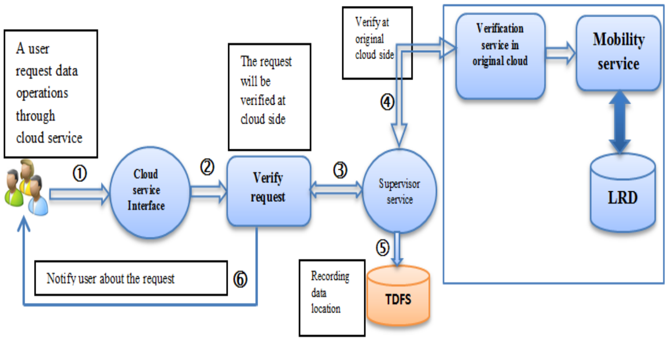

A user request data operations through cloud service
The request will be verified at cloud side
Verify at original cloud side
Verification service in original cloud
Mobility service
①
Cloud service Interface
②
Verify request
③
Supervisor service
④
LRD
⑤
Recording data location
TDFS
Notify user about the request
⑥

Fig. 9. Data mobility workflow

When the mobility service is triggered, it creates a request and sends it to the data operator where data location is queried at the LRD. Further, the data owner (if elected) will also be informed a message concerning the accessed operations via email or mobile devices. Details of the workflow are shown in figure 10.

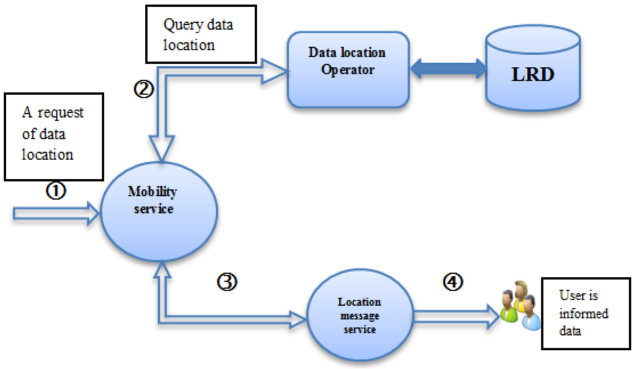


Fig. 10. Mobility service workflow

## VII. Evaluation and Results

### A. Experimentation setup

Our experimental environment has been set up as follows: Amazon EC2 [12] was used as the original cloud to provide cloud resources and verify requests. We created an instance of Windows 2012 server running on Intel Xeron E5-2670 v2 2.5GHz 2.5GHz 1GB. Packages of the model were deployed on this instance and requests were accessed via RMI interface. We also created another instance at Amazon EC2 running MySQL to store the LRD with 5 GB. Azure cloud [13] was used as the visited cloud. We created a virtual machine running Windows 2012 server 1.75GB AMD Opteron Processor 4171 HE 2.1 GHz to send requests via RMI interface. In order to demonstrate the working of the mobility model, a message application for notification at users' mobile phone was implemented in Java on an Android 4.4 smartphone with 3GB RAM and a 2400 MHz CPU. Google Cloud Message (GCM) [14] was devised to send messages informing users when the data was accessed or moved at cloud side. A notification could be triggered via two sources depending on the request of data operations. If the request was to move or to copy data, the mobility service would inform the data owner via GCM while operations such as read or write would be triggered by the probe inside the data.

The current experiments were based on following assumptions as they mainly focus on the mobility model: we assumed that the runtime environment (JVM) of the active data behaved correctly at participant clouds, and we assumed that the data would be activated when it moves to a new cloud host. We also assumed that a safe Location Service Provider (LSP) was available on the Internet and CSPs had the agreement to establish new supervisor. At this stage, we only tested our model on cases where TDFS and regular files were moved between two clouds.

### B. Evaluation

Since this work investigates a new data mobility model for ADCu, We first examined the time spent in the verification and identification and then measured the performance of our model. Components of the model were verified its functions which response accurately to a data moving requests such as verifying permissions, triggering an alter message, updating data location and informing user about data location. Furthermore, the experiments demonstrated the performance comparison between the operation on regular data files and ADCu in our model to prove that there was not too much the additional overhead when deploying the model within ADCu. The idea is to determine the overhead introduced by the security features and mobility service. We considered increasing the file size from 300KB to 1000KB for both TDFS and normal files (PDF files). The result of a request to move the data is shown in Table I. The executed time $t_{\text{Request}}$ for each request is composed of three determinants: the verification time $t_{\text{Lookup service}}$, the location register time $t_{\text{Verification and mobility}}$ and the data operation time $t_{\text{Data operation}}$

$$t_{\text{Request}} = t_{\text{Lookup service}} + t_{\text{Verification and mobility}} + t_{\text{Data operation}}$$

1) $t_{\text{Lookup service}}$ : is the time that client spent looking up server's RMI interface and sends the request.

2) $t_{\text{Verification and mobility}}$: is security and mobility service latency. The CPRBAC and Location register will be processed during this period.

3) $t_{\text{Data operation}}$: is the data transfer time between the original cloud and the visited cloud.

TABLE I. Data mobility processing time for moving the data

| File size (KB) | Average TDFS processing time (ms) $t_{\text{Request}}$ | | | | Average Normal file processing time (ms) $t_{\text{Request}}$ | | | |
|---|---|---|---|---|---|---|---|---|
| | $t_{\text{Lookup service}}$ | $t_{\text{Verification and mobility}}$ | $t_{\text{Data operation}}$ | **Total** | $t_{\text{Lookup service}}$ | $t_{\text{Verification and mobility}}$ | $t_{\text{Data operation}}$ | **Total** |
| **300** | 1467.4 | 595.2 | 1735.6 | **3798.2** | 1448.4 | 579.6 | 1708 | **3736** |
| **400** | 1486 | 589 | 1985.8 | **4060.8** | 1445.2 | 576 | 2006.2 | **4027.4** |
| **500** | 1452.2 | 601.6 | 2117.6 | **4171.4** | 1458.4 | 598 | 2074.8 | **4131.2** |
| **600** | 1452.8 | 579.8 | 2303 | **4335.6** | 1435.8 | 583.4 | 2243 | **4262.2** |
| **700** | 1470.8 | 579 | 2449.4 | **4499.2** | 1449.4 | 585.8 | 2475 | **4510.2** |
| **800** | 1458.4 | 595.8 | 2555.6 | **4609.8** | 1451.8 | 595.2 | 2546 | **4593** |
| **900** | 1435.8 | 582.6 | 2647.2 | **4665.6** | 1454.2 | 609.2 | 2727.2 | **4790.6** |
| **1000** | 1465 | 593.6 | 2781 | **4839.6** | 1450 | 587.8 | 2820 | **4857.8** |

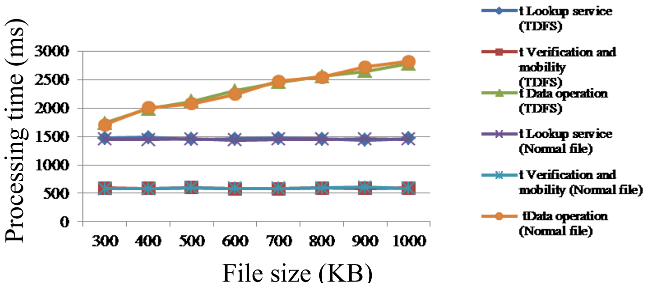


Fig. 11. Modules Processing Duration

From the results, it is clear that the processing time for TDFS is slightly more than that for normal files (4372.53ms in comparison with 4363.55ms of the later). The significant time contributes to the whole process are Lookup service time and moving data time since we deployed instances located at different clouds. The verification and mobility service time, the main process of the model, however, only constitutes small amount of time (589.58 of 4372.53ms for TDFS and 589.38 of 4363.55ms for Normal file respectively). The comparative result is also illustrated graphically in figure 11 and figure 12.

First, we identified the sources of delay such as verification time, the data transfer time and lookup service times. The experimental values on the verification time and lookup service of the model are approximately same for TDFS and normal file. Therefore, the source of delay could be introduced by the transfer time. So, we run the same request with different data sizes.

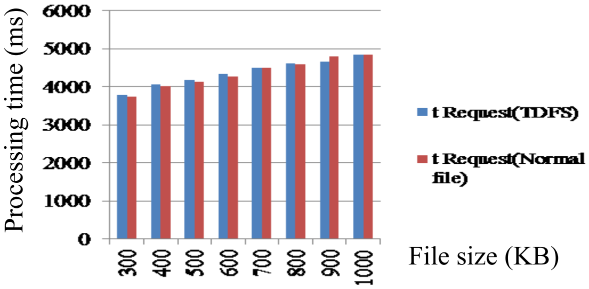
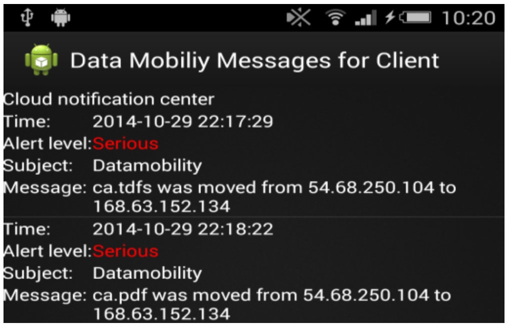


Fig. 12. Request Processing Duration



10:20

Data Mobiliy Messages for Client

Cloud notification center
Time: 2014-10-29 22:17:29
Alert level: Serious
Subject: Datamobility
Message: ca.tdfs was moved from 54.68.250.104 to 168.63.152.134
Time: 2014-10-29 22:18:22
Alert level: Serious
Subject: Datamobility
Message: ca.pdf was moved from 54.68.250.104 to 168.63.152.134

Fig. 13. Data notification view in SonyXperia Z2

The results show that the transfer data time is the significant source of latency. This means the data protection and mobility service are not the reasons for the introduced communication overhead. Even when the data size was increased from 300 KB to 1000 KB the verification overhead did not increase significantly.

Figure 13 shows alerting the messages to data owner via the mobile phone when there are requests to move the TDFS and regular file. It is demonstrated that the supervisor can detect invoke mobility service to send the alter message to user's mobile device immediately when there is a request to move the data at both original cloud and visited cloud.

## VIII. Conclusion and Future Work

This paper presented a data mobility management model for data mobility and data protection to enhance the exchange information among CSPs while ensuring users' controllability, traceability of data and authorized access to cloud resources under a fine-grained data protection scheme. It also proposed a novel LRD that is capable to serve for tracing and tracking data locations. Furthermore, a new TDFS structure with recordable structure was designed to actively capture locations of requests. More importantly, a proposed establishing supervisor at visited cloud is able to deploy the equivalence data protection scheme at both cloud side to achieve an intrusion tolerant scheme. The experimental outcomes demonstrate feasibility, efficiency of the model. Further, the reliability of the system is guaranteed in terms of processing time.

The future work will consider the deployment of more clouds for the data mobility model. In addition, different data operations, data moving cases and more requests will be experimented to evaluate performance and security of the system.

## References

[1] L. Schubert and K. Jeffery, "Advances in clouds," Report of the Cloud Computing Expert Working Group. European Commission, 2012.

[2] I. Foster, Z. Yong, I. Raicu, and L. Shiyong, "Cloud Computing and Grid Computing 360-Degree Compared," in Grid Computing Environments Workshop, 2008. GCE '08, 2008, pp. 1-10.

[3] T. Ries, V. Fusenig, C. Vilbois, and T. Engel, "Verification of Data Location in Cloud Networking," in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on, 2011, pp. 439-444.

[4] L. Chen and D. B. Hoang, "Addressing Data and User Mobility Challenges in the Cloud," in Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, 2013, pp. 549-556.

[5] D. Popa, K. Boudaoud, M. Borda, and M. Cremene, "Mobile cloud applications and traceability," in Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition, 2013, pp. 1-4.

[6] S. Betge-Brezetz, G. B. Kamga, M. P. Dupont, and A. Guesmi, "Privacy Control in Cloud VM File Systems," in Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on, 2013, pp. 276-280.

[7] N. Tcholtchev, B. Dittwald, T. Scheel, B. I. Zilci, D. Schmidt, P. Lammel, J. Jacobsen, and I. Schieferdecker, "The Concept of a Mobility Data Cloud: Design, Implementation and Trials," in Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International, 2014, pp. 192-198.

[8] L. Chen and D. B. Hoang, "Active data-centric framework for data protection in cloud environment," in ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012, 2012, pp. 1-11.

[9] L. Jae-Woo, "Mobility Management Using Frequently Visited Location Database," in Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on, 2007, pp. 159-163.

[10] L. Chen and D. B. Hoang, "Novel Data Protection Model in Healthcare Cloud," in High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on, 2011, pp. 550-555.

[11] L. Chen and D. B. Hoang, "Towards Scalable, Fine-Grained, Intrusion-Tolerant Data Protection Models for Healthcare Cloud," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on, 2011, pp. 126-133.

[12] A. EC2. (2014). Amazon Elastic Compute Cloud. Available: http://aws.amazon.com/

[13] Azure. (2014). Microsoft Azure. Available: https://azure.microsoft.com

[14] GCM. (2014). Google Cloud Messaging for Android. Available: https://developer.android.com/google/gcm/index.html