UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

Agents-based Security Model for Cloud Database Applications

BY

MOURICE GUYA

P58/75964/2012

SUPERVISOR

MR. CHRISTOPHER MOTURI

September 2014

A project report submitted in partial fulfillment for the requirements of Master of Science in Computer Science of the University of Nairobi

Declaration

The project report presented in this report is my original work and has not been presented for any other university award.

Signature _____ Date _____

Mourice Guya (P58/75964/2012)

This project has been submitted in partial fulfillment of the requirements of the Master of Science in Computer Science of the University of Nairobi with my approval as the University supervisor.

Signature _____ Date _____

Mr. Christopher Moturi

Deputy Director

School of Computing and Informatics

Acknowledgement

"But we have this treasure in jars of clay to show that this all-surpassing power is from God and not from us" 2cor 4:7

I am grateful to my supervisor Mr. Christopher Moturi for providing direction throughout this project. I also acknowledge valid criticism and directions offered by panelists Dr. Agnes Wausi, Mr. Evans Miriti and Mr. Samuel Ruhiu. Criticism engineered pragmatism that brought this refined piece work. Thanks to all research data source stakeholders for availing the needed information.

Dedication

I would like to dedicate this project to my wife Mrs. Judy Guya, daughters Faith, Connie, Abby and son Joseph for providing complete inspirational environment that made this a success. I am grateful for the spiritual and material support from my wife that made me to start and complete this course.

Abstract

Cloud computing offers a number of benefits but security challenges has remained a big barrier for its widespread applications**.** As cloud computing moves the application software and databases to be hosted by third parties, the management of such data and services becomes untrustworthy. The security challenges include unauthorized access, reduced control over data, over reliance on service providers and encryption performance degradation. This study sought to explore security techniques in current research works; identify cloud security challenges amongst users and cloud providers in Nairobi, Kenya; and develop and test an agent-based cloud security model. Findings from different research works revealed encryption having performance degradation issues, no real time data monitoring tool for clients, and data residing in one storage location and can easily be accessed upon intrusion. Sample population from financial sector and cloud service providers were used for the study. A multi-agent cloud security model was developed, using the Prometheus multi-agent methodology, to provide a combined and intelligent security solution. Research findings revealed concerns over cloud security and this model provides the needed solution encompassing data classification and separation, selective encryption, access control, use of agents to search and update massive volumes of data, and real-real time monitoring. Data classification and separation allows data to be kept at different location thereby making data incomplete upon intrusion whereas selective encryption minimizes the volume of data to be encrypted thereby reducing encryption and decryption performance degradation.

Table of Contents

List of Figures

List of Tables

Abbreviations

NIST	National Institute of Standards and Technology
SPI	Software as a service, Platform as a service and Infrastructure as a service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
CapEx	Capital Expense
OpEx	Operational Expense
CRM	Customer Relationship Management
CSP	Cloud Service Provider
APIs	Application Program Interfaces
CSA	Cloud Security Alliance
CNBC	Consumer News and Business Channel
DMTF	Distributed Management Task Force
ITU	International Telecommunication Union
ENISA	European Network and Information Security Agency
CCSW	Cloud Computing Security Workshop
SCC	Secure Cloud Computing
IARIA	International Academy, Research and Industry Association
AES	Advanced Encryption System
SSL	Secure Socket Layer
FHE	Fully Homomorphic Encryption
CCSW	Cloud Computing Security Workshop
SCC	Secure Cloud Computing
HDFS	Hadoop Distributed File System
MAS	Multi-Agent Systems
CDS	Cloud Data Storage
JADE	Java Agent Development Environment

Definition of Terms

Encryption - Process of encoding messages or information

Decryption - Process of transforming data to un-encrypted form

ICloud - Cloud storage and cloud computing service from Apple Inc

Dropbox - Cloud storage service for file sharing offered by Dropbox Company

Google drive - File storage and synchronization service provided by Google

Method - Particular procedure for accomplishing something

Model - Representation of an object or part of the world

Technique - Systematic method based upon logic

Framework - Skeleton of interlinked items

Homomorphic Encryption - Carrying operations on encrypted data without decryption

Multi-tenancy - Resource assigned to multiple users.

CHAPTER ONE
INTRODUCTION

1.1 Background

National Institute of Standards and Technology (NIST) defines cloud computing as "cloud computing is a model for enabling ubiquitous, 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 promotes availability and comprised of five key characteristics, three delivery models and four deployment models. The key characteristics of clouds are: on demand self service, ubiquitous network access, location independent resource pooling, rapid elasticity and pay per use. A commonly agreed framework describing cloud computing services goes by the acronym "SPI"(Mather, Kumaraswamy & Latif, 2008). Fig 1 shows SPI framework

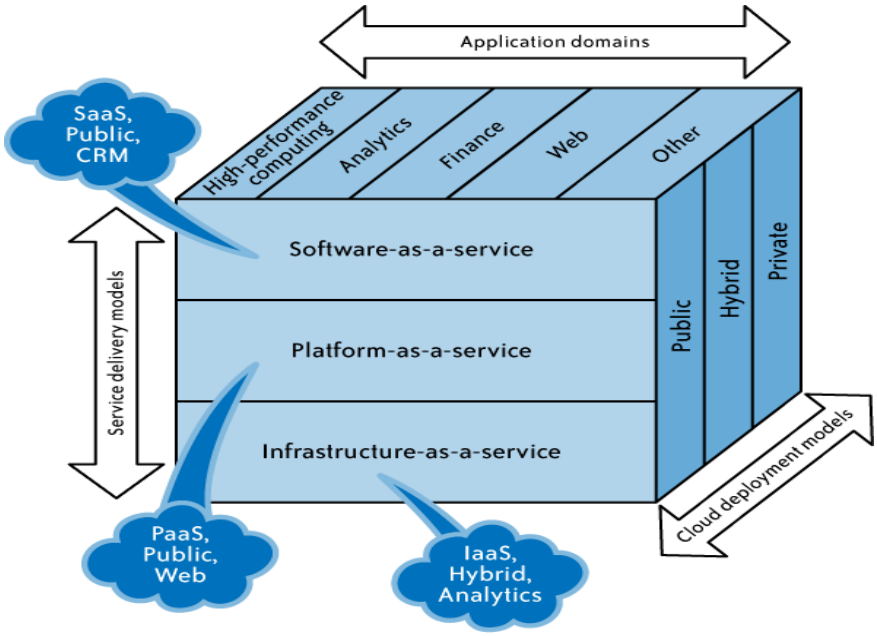


Figure 1: SPI Framework: Source (Mather et al, 2008)

Cloud computing consist of cloud deployment and service delivery models (Ritesh, Swati & Chatur, 2012; Pearson, 2012; Mather, Kumaraswamy & Latif 2008). The deployment and service delivery models pose different security challenges.

Cloud Deployment Models and Challenges

This represents specific type of cloud environment, the various deployment models have different security issues (El-khameesy & Rahman, 2012).The four deployment models are:-

i) Public Clouds - Is based on massive scale offerings to the general public. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure. They offer greatest level of efficiency in shared resources however they are more vulnerable.
ii) Private clouds - The cloud infrastructure is owned or leased by a single organization and is operated only for that organization. Offers the greatest level of security and control but still require the company to purchase and maintain all the software and infrastructure.
iii) Community clouds - Provide shared infrastructure for a specific community that has shared concerns e.g. compliance issues.
iv) Hybrid clouds - Hybrid clouds are a combination of public, private, and community clouds.

Cloud Service Delivery Models and Challenges

Entails how services are delivered via the cloud, Cloud computing is used to sell hosted services in the sense of application service provisioning that run client server software at a remote location. End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. IaaS is the foundation of all cloud services followed by PaaS then SaaS. Just as capabilities are inherited, so are the information security issues and risks (Kavitha & Subashini, 2010). Each service has its own security issues (Kandukuri, Paturi & Rakshit, 2009). Such delivery models include:

i) Infrastructure-as-a-service (IaaS) - The IaaS service model is the lowest service in the technology stack, offering infrastructure resources as a service, such as data storage, processing power and network capacity. The consumer can use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than PaaS and SaaS. The consumer does not manage or control the underlying cloud infrastructure; provider is in complete control of the infrastructure and what runs in it (Ritesh, Swati & Chatur, 2012). IaaS is prone to various degrees of security issues based on the cloud deployment used; Public cloud poses the major risk. Examples include Amazon EC2, S3.

ii) Platform-as-a-service (PaaS) - The vendor offers a development environment to application developers, who develop applications and offer those services through the provider's platform. The consumer does not manage or control the underlying cloud

infrastructure including network, servers, operating systems or storage but has control over deployed applications (Ritesh, Swati & Chatur, 2012). PaaS is a variation of SaaS whereby the development environment is offered as a service. Examples include Google Aps, Force.com and Microsoft Azure.

iii) Software as a service (SaaS**)** - Traditional methods of purchasing software involved the customer loading the software onto his own hardware in return for a license fee (*CapEx*). In IaaS, customer does not purchase software, but rather rents it for use on a subscription or pay-per-use model (*OpEx*). Typically, the purchased service is complete from a hardware, software, and support perspective. Examples Salesforce CRM, GoogleDocs, etc. The client has to depend on the provider for proper security measures. The provider must do the work to keep multiple users' from seeing each other's data; it becomes difficult to the user to ensure that right security measures are in place (Choudhary, 2007). Fig 2. Shows the various cloud service delivery layers, Fig 3. Shows what cloud provider controls in different service delivery models (Mather, Kumaraswamy & Latif, 2008)

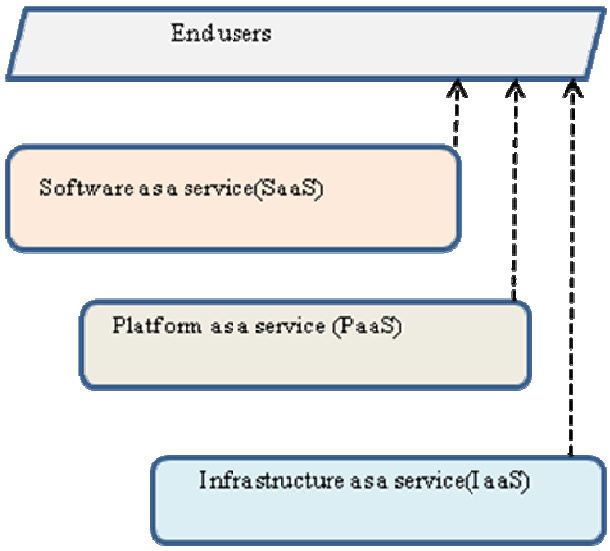


Figure 2: Cloud service delivery layers: Source (Pearson, 2012)

Layer	Service model		
	Software as a service	Platform as a service	Infrastructure as a service
Facility	✓	✓	✓
Network	✓	✓	✓
Hardware	✓	✓	✓
OS	✓	✓	?
Middleware	✓	?	—
Application	✓	—	—
User	—	—	—

* Question marks indicate layers in which either the provider or user could be in control.

Figure 3: Cloud service delivery layers: Source (Pearson, 2012)

1.2 Problem Definition

Cloud computing provides a number of benefits however cloud security is always a hindrance and a big barrier for its widespread applications. As cloud computing moves the application software and databases to third party infrastructure, the management of the data and services becomes untrustworthy (El-khameesy & Rahman, 2012). Each service has its own security issues (Kandukuri et al., 2009). A key problem in outsourcing the storage and processing of data is that parts of the data may be sensitive, such as business secrets, credit card numbers, or other personal information. Storing and processing sensitive data on infrastructure provided by a third party increases the risk of unauthorized disclosure if the infrastructure is compromised by an adversary (who could be an insider from the third party provider).Some of the security challenges are :-

i) Unauthorized access -compromising data integrity and confidentiality(Pearson, 2012)
ii) Lack of user control/loss of control over data (Pearson, 2012)
iii) Over reliance on service providers (Choudhary, 2007) e.g. Data migration being carried by Service provider, Violation of SLA
iv) Encryption performance degradation (Weis & Alves - Foss, 2011; Chen,2012)
v) Encryption key management problem (Balding,2008; Chen, 2012)

1.3 Objectives

The aim of this project was to develop an agent-based security model for database applications that combines different cloud security approaches together with add on functionalities. The following were the objectives of the study:-

1. Explore existing cloud security techniques, methods and models in current research works
2. Identify cloud data security techniques being used by sampled Nairobi cloud providers and sampled users within Financial Sector
3. Develop agent-based cloud data security model for database applications
4. Test and validate the agent-based cloud data security model

1.4 Research Questions

The following are the research questions that guided the study:-

1. What are the cloud security techniques in current research works?
2. What are cloud security techniques being used by Nairobi cloud providers?
3. Are ICT data custodians and managers within financial sector like Pension, Banking and Insurance industries aware of cloud computing? Are they aware of cloud computing security?
4. Which method allows users to be in control of their data and also makes data valueless upon intrusion?
5. Is there a model that can combine the different security approaches?
6. Is agent-based cloud security model appropriate?

1.5 Scope of the Study

The study focused on cloud security model for database applications covering security challenges, access controls, data classification, data manipulations, events logs and monitoring, selective encryption, security analysis and reporting. Cloud computing security broadly falls under management, operations and technology (Mitchell & Alcock, 2010). The rest of technology class such as identity and key management, backup and restorations, audit and compliance, physical security and network protection have been left out for now. The model does not cover other cloud storage services like iCloud, dropbox. The study was limited to financial institutions since they are major leaders in technology usage and they also deal with large financial transactions that are sensitive and susceptible to fraud.

1.6 Significance of the Study

Cloud computing opens up a new world of opportunities but faces numerous security challenges that need to be considered and addressed .This project explored the various cloud computing security techniques so as to establish a combined security model that protects data and allow customers to have control over their data thereby increasing trust, confidence and uptake of cloud services. Omwansa,Waema,Omwenga (2014) observed that 50% of South Africa's medium and large businesses were using cloud services, compared to 48% in Kenya and 36% in Nigeria, This means Kenya have already identified the cloud computing potential and this model will significantly increase cloud uptake.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

Cloud Computing uptake in Kenya

Omwansa, Waema, Omwenga (2014) on their 2013 cloud baseline survey pointed out that cloud usage in Kenya is at 48% however there is need to: - Enhance the awareness of cloud technologies, Develop national cloud computing strategy, Enhance cyber security, Enhance the relevant legal and regulatory frameworks. Their key findings on awareness showed low awareness as majority of respondents (80%) were not aware of either policy or legal frameworks, 75% of respondents indicated they were not aware of any cloud computing standards. A survey done by Ovum in Kenya in 2012 found out that 47% of organizations were already using cloud systems for corporate IT systems. Kituku (2012) observed that privacy and security had affected adoption of cloud computing by companies listed at Nairobi Stock Exchange.

Cloud Computing uptake in Africa

Africa still lags behind in cloud uptake. As of 2012, all countries surveyed indicated that cloud computing was being considered. The study targeted all South Sahara African countries. Twenty-five countries were surveyed. The study revealed that in 68% of the countries surveyed, the government administration was at the stage of studying the introduction of cloud computing. 11% were piloting, 16% implementing while 5% were already using (Omwansa, Waema, Omwenga, 2014).

African countries have introduced cloud computing at different levels according to a study conducted by International Telecommunication Union (ITU) in 2012 however ITU recommended: - a regulatory approach that caters for security/confidentiality and personal data protection, Network connection security, Data protection, Certification of CSPs amongst others.

Cloud Computing security -world wide

A number of computing groups have announced their efforts to promote some facet of cloud computing. Some of these groups are:- NIST,CSA,ENISA,IARIA,CCSW,SCC,DMTF, Jericho Forum(an international information security thought leadership association) among

many others. There has been significant research work in cloud computing and cloud computing security over the years. Several groups and organizations are interested in developing security solution and standards for the cloud. Cloud Security Alliance (CSA) is at the forefront in gathering solution providers to foster current and future best practices for information assurance in the cloud.

IARIA held the fifth International Conference on Cloud Computing, GRIDs and Virtualization at Venice, Italy on May 25-29, 2014. One of the topics was cloud security challenges and solution discussions on:-Privacy, Load balancing, Agent-based cloud computing amongst others.

CSA, ENISA and Fraunhofer-FOKUS joined forces and held the third edition of the Secure Cloud conference at Amsterdam in April 2014 that focused on legal issues, cryptography, incident reporting, certification and compliance.

CSA organized fifth CSA Summit held at San Francisco in February 2014 where key policy makers and industry luminaries discussed industry's seminal issue (" can we trust global cloud service providers to protect customers located anywhere in the world ?").

Cloud computing security workshop (CCSW) held at Berlin in November 2013 focused on cloud centric security focusing on practical cryptography for cloud security, secure cloud resource virtualization based on access controls, cloud aware web services security paradigm, scalability of security in global size clouds and security for cloud programming models.

Secure Cloud Computing(SCC) held International Workshop on Secure Cloud Computing at Xian, China in September 2013 which focused on the security infrastructure and framework of cloud computing, Coding and cryptography for secure cloud, Distributed computation and access control on encrypted data, Privacy preserving technologies in cloud computing, Secure data sharing, secure data replication and Secure data synchronization.

2.2 Limitations of existing Techniques, Models and Methods

2.2.1 Techniques

i) Encryption

Data security in the cloud is one of the biggest issues. To protect data, use of Advanced Encryption Standard (AES) and Secure Socket Layer is proposed (Darsi, Suresh, Jayakumar, 2012). AES is used to encrypt data in the cloud and SSL is used to secure transfer of data over the internet.

Encryption Key Management Problems

The common solution for data confidentiality is data encryption. Encryption brings key management problem and performance degradation. Who is responsible for key management? Ideally, it's the data owners. But at present, because the users have not enough expertise to manage the keys and lack of security awareness, they usually entrust the key management to the cloud providers. As the cloud providers need to maintain keys for a large number of users, key management becomes more complex and difficult (Chen, Zhao, 2012). Since much of Cloud Computing is based on replication, it is important to maintain the distinctiveness of encryption and decryption keys. Recently, Amazon faced a challenge with this issue on their Cloud systems (Balding, C. 2008). The main issues are: - General security issues e.g. Keys being stolen, Keys being vulnerable to attack or compromise. Management of keys problem e.g. Single point of failure, Need to scale linearly to handle lots of keys

Encryption Performance Problem

Encryption seems like the perfect solution for ensuring data security; however, it is not without its drawbacks. Encryption takes considerably more computational power, and this is multiplied by several factors in the case of databases (Weis & Alves-Foss, 2011). Cryptography greatly affects database performance because each time a query is run, a large amount of data must be decrypted; and since the main operation on a database is running queries, the amount of decryption operations quickly become excessive. As the cloud computing environment involving large amounts of data transmission, storage and handling, there is effect on processing speed and computational efficiency. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. For the static data used by cloud-based applications in PaaS or SaaS model, data encryption in many cases is not feasible because data encryption would prevent indexing or searching of that data, the static data used by Cloud-based applications is generally not encrypted. Not only in cloud, but also in traditional IT environment, the data being treated is almost not encrypted for any program to deal with it (Chen et al., 2012; Mather et al., 2008).

ii) Homomorphic Encryption

In June 2009, IBM developed a fully homomorphic encryption(FHE) scheme which allows computation to be done on encrypted data without decrypting data however it requires immense computation effort. Gentry the IBM researcher estimates that performing a simple google search with encrypted keyword with this algorithm would increase amount of computing time by about a trillion. Successful adoption of FHE for query processing is, however, still a distant dream, and numerous challenges have to be addressed. One challenge is how to perform algebraic query processing of encrypted data, where we produce encrypted

intermediate results and operations on encrypted data can be composed (Mani, Shah and Gunda, 2013). Conceptually, an FHE scheme can evaluate any function, and hence can process any query. However, applying FHE to query processing is not straightforward, and several issues have to be addressed. The first one is how to translate any query into a FHE circuit that can be evaluated on encrypted data.

iii) Anonymization

Anonymization technologies such as K anonymous and data pre-processing methods faced challenges when applied to large data (Mulero, 2009).

2.2.2 Models

i) Three Level Defense Model

By analyzing HDFS, (Yuefa et al, 2009) developed security model anchored on three level defense systems namely:-

a) The first layer- Responsible for user authentication, digital certificates issued by the appropriate, manage user permissions.
b) The second layer-Responsible for user's data encryption, and protect the privacy of users
c) The third layer: The user data for fast recovery.

With three-level structure, user authentication is used to ensure that data is not tampered with though it does not provide data separation, selective encryption and monitoring mechanisms

ii) Two Phase Model

Darsi et al., (2013) proposed a two phase model structured to provides security to the data in the entire process of cloud computing, be in transit or in cloud. The model divided into two phases, First Phase deals with the data encryption, and secure transfer data over internet. Second Phase deals with the data retrieval from cloud, includes the decryption process and double authentication process, one by owner/company and another by cloud service provider. This model is susceptible to encryption and performance degradation and there is also key management problem in which dishonest providers can use the client data for financial gain.

iii) Jericho Model

Ritesh, Swati & Chatur (2012) Jericho Forum's Cloud Cube Model provides a figuration description of security attribute information implied in the service and deployment models of cloud computing and the location, manager and owner of computing resources. The definitions of model parameters are as follows:

a) Internal/External: a model parameter to define the physical location of data storage. If the physical location of data storage is inside of the data owner's boundary, then the model parameter value is internal. Contrariwise, the model parameter value is external.
b) Proprietary/Open: a model parameter to define the ownership of cloud's technology, service and interface etc. This model parameter indicates the degree of interoperability, i.e. the portability of data and application between proprietary system and other cloud modalities, the ability of transforming data from a cloud modality to other cloud modality without any constraint.
c) Perimeterised/De-perimeterised: a model parameter to describe the "architectural mindset" of security protection, i.e. a customer's application is inside or outside of traditional security boundary? Perimeterised means that a customer's application operates within traditional IT security boundary signaled by firewall (Ritesh et al., 2012).
d) Insourced/Outsourced: a model parameter to define the 4th dimension that has two states in each of the eight cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO). Insourced means that cloud service is presented by an organization's own employees, and Outsourced means that cloud service is presented by a third party. These two states answer the question "who do you want to build or manage your cloud service?" This is a policy issue (i.e. a business but not a technical or architectural decision).

   Jericho model gives out mini framework to be considered.

iv) **Cloud Risk Accumulation**

The cloud risk accumulation model is based on understanding of the layer dependency of cloud service models in order to analyze the security risks of cloud computing. IaaS is the foundation layer of all cloud services, PaaS is build upon IaaS and SaaS is built upon PaaS, so there is inherited relation between the service capability of different layers in cloud computing. Similar to the inheritance of cloud service capability, the security risks of cloud computing is also inherited between different service layers (Ritesh et al., 2012).This model only explains the risk dependency between layers.

2.2.3 Methods

i) Security -As-a-[Cloud] Service Method

Just like software-as-a-service (SaaS), the business model with security-as-a-service is subscription-based. In addition, security-as-a-service is also sometimes referred to as "SaaS". With SaaS, there are two emerging provider types. The first type comprises established information security vendors who are changing their delivery methods to include services delivered through the cloud. The second type comprises start-up information security

companies that provide security only as a cloud service, and do not provide traditional client/server security products for networks, hosts, and/or applications (Mather et al., 2008). Such service includes email filtering, web content filtering, vulnerability management, identity management etc. Under this, cloud client is still under the mercy of the cloud security provider.

ii) Agent Methods

One key feature of software agents is the intelligence that can be embodied into them according to some collective artificial intelligence approach that needs cooperation among several agents that can run on a parallel or distributed computer to achieve the needed high performance for solving large complex problems keeping execution time low.

In large-scale data centers, agents can search, filter, query and update the massive volumes of data that are stored. We can envision a scenario where cloud agents working on our and operating systems behalf, to provide intelligent data access services, monitoring services, processor-to-application assignment strategies, and energy-efficient use of Cloud computing infrastructures(Talia,2011).

A theoretical approach of security framework as well as a MAS architecture (Talib, 2010) that could be implemented in cloud platform in order to facilitate security of CDS, on how the MAS technology could be utilized in a cloud platform for serving the security that is developed by using collaborative environment of JADE.

The MAS composed of five types of agents User Interface Agent (UIA), User Agent (UA), DER Agent (DERA), Data Retrieval Agent (DRA) and Data Distribution Preparation Agent (DDPA). The agent functions are as follows:-

i) UIA- Considered as the main and leader agent, this agent is acts as an effective bridge between the user and the rest of the agents. Such agents actively assist a cloud user in operating an interactive interface, recording the messages and data shared among agents and also serves as a data access point for other agents, as well as cloud users.
ii) DDPA - Used to tolerate multiple failures in distributed CDS systems. In CDS, we rely on this agent to disperse the data file redundantly across a set of distributed servers. The main goal of this agent is to generate a correctness security policy to secure the CDS.
iii) DRA -*:* Used to enable the cloud user to reconstruct the original data by downloading the data vectors from the servers. The main goal of this agent is to generate integrity security policy to secure the CDS.
iv) UA - Act as a customer gateway that makes features of MAS accessible to cloud users. It includes responsibility of providing cloud users with real-time information of entities

residing in the MAS. User agent also allows cloud users to control the status of loads based on priority predefined by a cloud user. The main goal of this agent is to generate both confidentially and integrity security policies to secure the CDS.

v) DERA -*:* Responsible for storing associated DER information, DER information to be stored may include DER identification number, type, local fuel availability, cost function or price at which cloud users agree to sell, as well as DER availability. The main goal of this agent is to generate availability security policy to secure the CDS.

This agent method does not provide: - data classification, access control, encryption, real-time monitor and data manipulation operations like query, search, update etc.

Rasim & Fargana (2013) proposed use of agent based federated identity management comprising of Service providers, Identity providers and Users. Idm comprises;-

i) Provisioning: the practice of provisioning of identities within an organization addresses the provisioning and deprovisioning of several types of user accounts (e.g. end user, the application administrator, IT administrator, supervisor, developer, etc).

ii) Authentication*:* the process of ensuring that the individual is who he claims to be, and is identified through various mechanisms, such as login, password, biometrics, token, etc.

iii) Authorization*:* a common need in security to provide different access levels (e.g. deny/allow) for different parts or operations within a computing system. This need is called authorization.

iv) Federation*:* a group of organizations or CSPs that establish a circle of trust that allows the sharing of information of user identities to each other.

This agent method does not provide data classification, encryption, real-time monitor and data manipulation like search, updates.

iii) Data Classification and Separation

The challenges in privacy protection are sharing data while protecting personal information. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. These concerns include whether personal information can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data elements (Chen, 2012*).* This does not provide encryption, real-time monitoring and access controls.

iv) SLA specification

The security SLA specifications and objectives related to data locations, segregation and data recovery has also been fronted (Kandukuri et al., 2009). This is prone to violations by the Cloud Service providers.

v) Cloud Security focus

After analyzing the management process disciplines across the ITIL and ISO frameworks (Mather et al.2008, p.133) identified the following relevant processes as the recommended security management focus areas for securing services in the cloud: Availability management (ITIL), Access control (ISO/IEC 27002, ITIL), Vulnerability management (ISO/IEC 27002), Patch management (ITIL),Configuration management (ITIL),Incident response (ISO/IEC 27002). This method lacks data separation and real-time monitoring.

2.3 Proposed Solution

Having explored the different research works, encryption and decryption have performance degradation issue due to voluminous nature of cloud data thus there is need for a model that provides selective encryption. It's also evident that complete data is kept in one place e.g. a particular database kept in one server in one particular place thus data is easily accessible upon successful intrusion, there is need to separate and store data in different locations. None of the models/techniques/methods have addressed the issue of real-time data monitoring on the client side. Cloud security calls for intelligence and combination of different security approaches. Cloud computing and multi-agent systems are distributed computing models thus multi-agents can be easily be used to provide combined and intelligent solutions to cloud environment. This project is a combined security model and a further work and implementation of data classification and separation proposal(Chen,2012), Access control(Yuefa et al,2009) ,Use of agents in cloud security(Talib,2010) , Use of agents to search, filter, query and update the massive volumes of data (Talia, 2011),*Use of* encryption (Darsi et al,2013) with addition of real time data monitoring . The model minimizes volume of data to be encrypted as it does selective encryption. It consists of:-

i) Data

ii) Agents: handles user interface, Views, Data manipulations, Data classification, Encryption, Anomaly monitoring, access controls and security analysis

CHAPTER THREE
METHODOLOGY

3.1 Introduction

This chapter sets out the research methodology that was adopted so as to meet the objectives of outlined in section 1.3. The chapter covers the research design, population sample, model design methodology, data collection and analysis.

3.2 Research Design

The research design type adopted was survey and prototype development. Survey was done in order to find out cloud security challenges amongst the stakeholders. Prototype was then designed to offer solution to various security challenges.

3.3 Population Sample

To identify respondents for the study, a stakeholder analysis was done that resulted in categorization of stakeholders: Cloud Service Providers, Users-Managers (Those who can influence cloud adoption), and Users-Custodians (Who are data custodians within clients' companies). Cloud users were drawn from financial sector population since they are major leaders in technology usage and they also carry large financial transactions that are sensitive and susceptible to intrusion. 10 user organizations and 3 cloud service provider organizations were identified who could participate in the study. Of the 10 user companies, 35 managers and 30 data custodians were targeted. Table 1 shows stakeholder categorization and sample.

Table 1: Stakeholder Categorization and sample

Category	Target users	Target Number of companies
1. Cloud Service Providers(CSP)	3	3
2. Users		
Users-managers	35	10
Users (DBA, SA, System security administrators)	30	10

3.4 Data Collection

Questionnaires were used to collect primary data. Different questionnaires were designed based on stakeholder groupings. Secondary data sources included journals, conference

proceedings and policy papers. Primary data was collected using a questionnaire with close ended and open ended questions. The questionnaires were administered to the selected staff of the target companies. All the 3 service provider companies responded, 32 out of 35 managers responded, 24 out of 30 and 7 out of 10 users' companies responded. Table 2 shows the number of respondents (*Refer to Appendix 1 for different set of Questionnaires)*

Table 2: Number of Respondents

Category	**Target population**	**Respondents**	**Number of companies that responded**
1. Cloud Service Providers(CSP)	3	3	3 out of 3
2. Users			
Users-managers	35	32	7 out of 10
Users (DBA, SA, System security administrators)	30	24	7 out of 10

3.5 Data Analysis

The nature of questions and data collection methods used necessitated the use of both qualitative and quantitative analysis methods. Qualitative analysis was done on open ended questionnaires which were later analyzed through quantitative techniques and interpretation given. Quantitative analysis entailed analysis of data in numerical form showing numerical counts, percentages, charts and graphs. Analysis was done at two levels: - i) Analysis based on data collection tools - Analysis on data obtained from data collection from questionnaires. ii) Analysis on the model performance based on results.

3.6 Multi-Agent Methodology

The model was developed using Prometheus methodology because it is detailed. MAScommonKADS was used for Analysis, Development and Testing. JAVA language was used for the development and Oracle VM was used for setting up of virtual machines. Fig 4. Shows Prometheus methodology

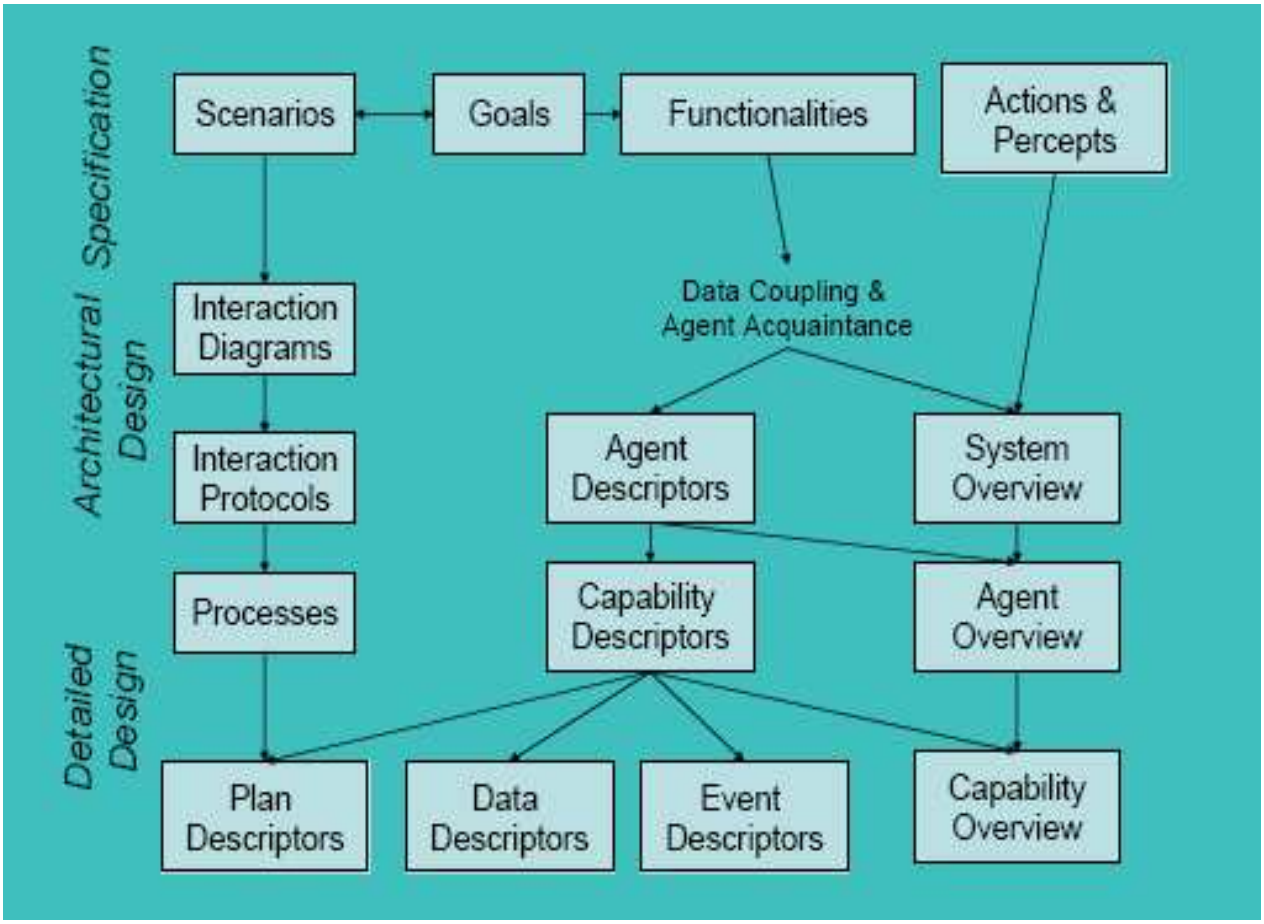


Figure 4: Prometheus Methodology: Source (Padgham, Winikoff, 2004)

CHAPTER FOUR
RESULTS AND DISCUSSIONS

4.1 Research Findings and Analysis

i) Findings from Cloud service providers

Figure 5 Shows security analysis by cloud service providers (*Refer to Appendix 2 for Cloud Service providers' questionnaire analysis)*

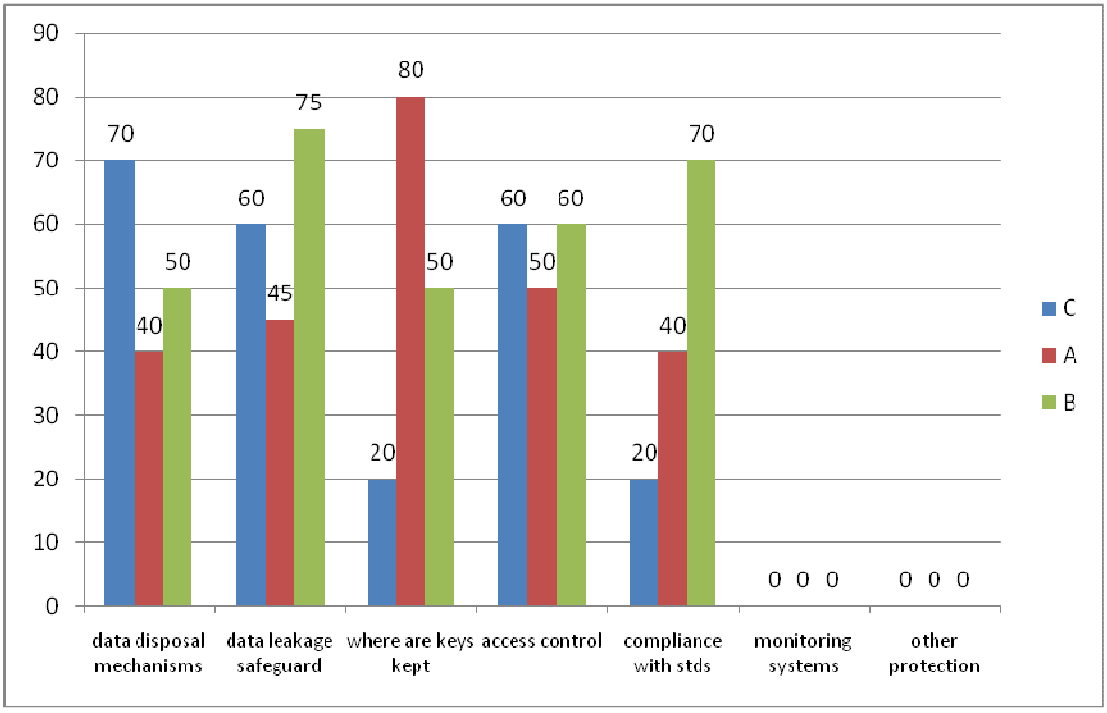


Figure 5: Key Security Analysis by Cloud service providers

Key findings

The following were specific findings: Encryption was the only protection mechanism, No provision of monitoring systems, Low compliance with industry standards and CSP not availing vital information to clients on issues of encryption key management

ii) Key findings from Managers

Table 3 shows key findings from managers and Figure 6 Shows security analysis by Managers.

Table 3: Findings from Managers

Key Question	Respondents	Total respondents	%
Does not know about cloud	4	32	12.5
Security Concerns	25	32	78
No cloud in Org. strategy	28	32	87.5
Cloud as costly	3	32	9
No control over cloud data	19	32	59
Cloud data owned by provider	20	32	62.5
Does not know cloud compliance standards	23	32	71.8
No recovery plan	22	32	68.7
No assurance mechanisms	26	32	81.25

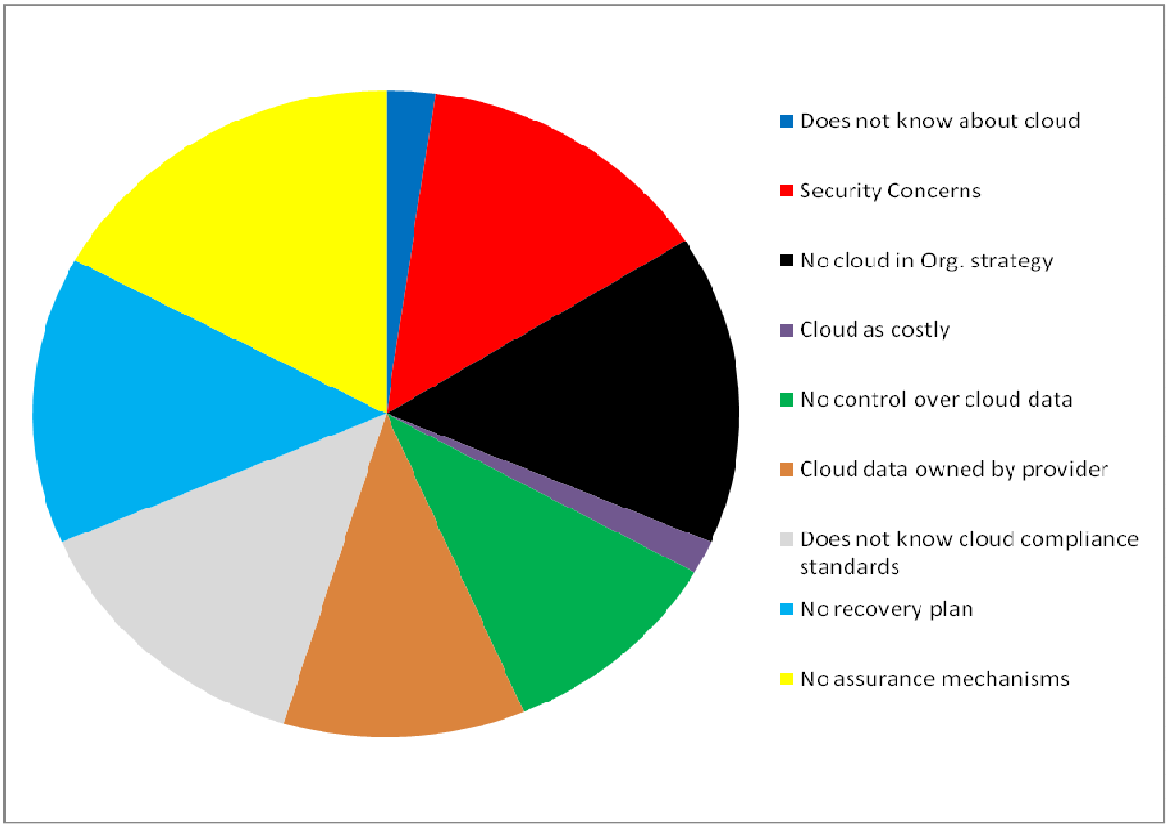


Figure 6: Security Analysis by Managers

Key findings

The following were specific findings:- 12.5% does not know about cloud, 78% had security concerns over the cloud ,87.5% had not incorporated cloud in their organizational strategy,81% had no assurance information from CSP, 62.5% believed their cloud data is owned by CSP, 59.5% believed there was no control over cloud data(*Refer to Appendix 3 for managers' questionnaire analysis)*

iii) Key findings from DBAs, SA, and System Security Administrators

Table 4 shows key findings from DBAs, SA, System Security Administrators and Fig. 7. Security analysis by DBAs, SA, System Security Administrators

Table 4: Key Findings from DBAs, System Administrator, System Security Administrators

Key Question	Respondents	%
Security concerns	22	91.6
Protection only by encryption	24	100
Monitoring as way of ensuring control	5	16.6
Data separation as a security option	0	0
Data migration done by cloud service provider	17	70.8

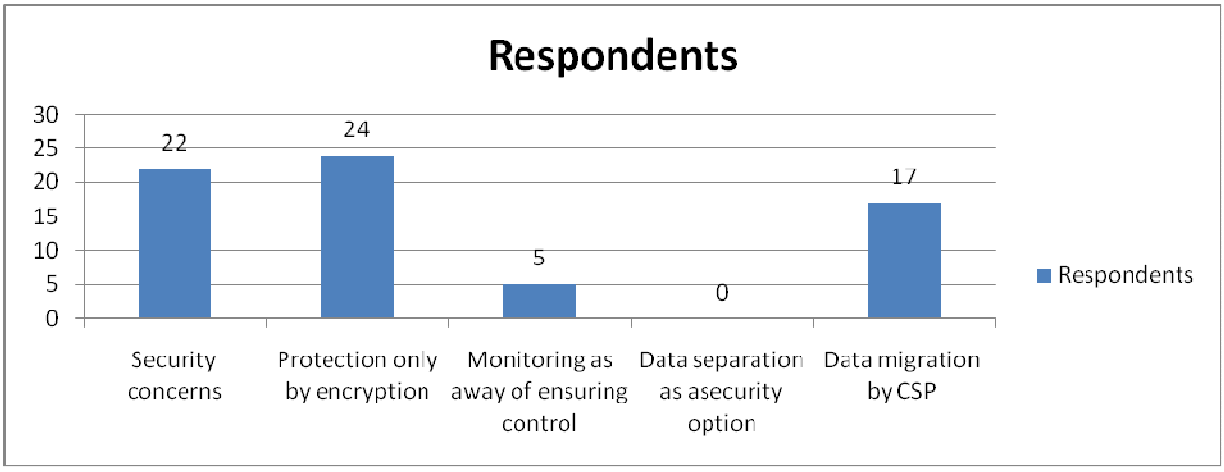


Figure 7: Security analysis by DBAs, SA, and System Security Administrators

Key findings

The following were specific findings:- 91.5% had security concerns over cloud,100% believed encryption was the only protection mechanism,100% believed in having access control so as to have control over their data,70% allowed cloud providers to carry data migration for them

(Refer to Appendix 4 for DBAs, SA, and System Security Administrators questionnaires' analysis)

4.2 Model Specification

Table 5 shows model action areas

Table 5: Model action areas

Stake holder	Problem	Action Model
Cloud Users	Reduced control/lack of control over user data	Real time Monitoring
	Security- Unauthorized access	Access control, monitoring, data separation, Security violation prevention
	Encryption as the only protection mechanism(encryption leads to performance degradation)	-Data separation -Encryption on sensitive data
	Security- lack of vulnerability assessments	Analysis reports for decision making
	SLA Violations	Monitoring
CSPs	Encryption as the only protection mechanism	Data separation, Encryption on sensitive data
	Lack of monitoring system	Monitoring

Analysis of users' problems revealed lack of alternate protection mechanism apart from encryption, unauthorized access upon intrusion, lack of real-time monitor, low security awareness, lack of security analysis reports. Table 6 shows Model Agents and Functions

Table 6: Model Agents and Functions

Agent Name	Functions
Interface	Provide interface where users can interact with the system
Data Separation	Performs data classification and store data in different locations
Real-time monitor	Keep logs of anomalies and provide real-time monitoring
Access control Agent	Provide and enforce access controls
Data manipulation agents	Performs Updates, Inserts, Deletions, Search, Views
Analysis agents	Provide vulnerability/security reports
Encryption	Performs encryption only on sensitive data

4.3 Model Design

Architectural and detailed designed was carried out.

4.3.1 Architectural Design

The system overall structure was designed as shown in Fig. 8

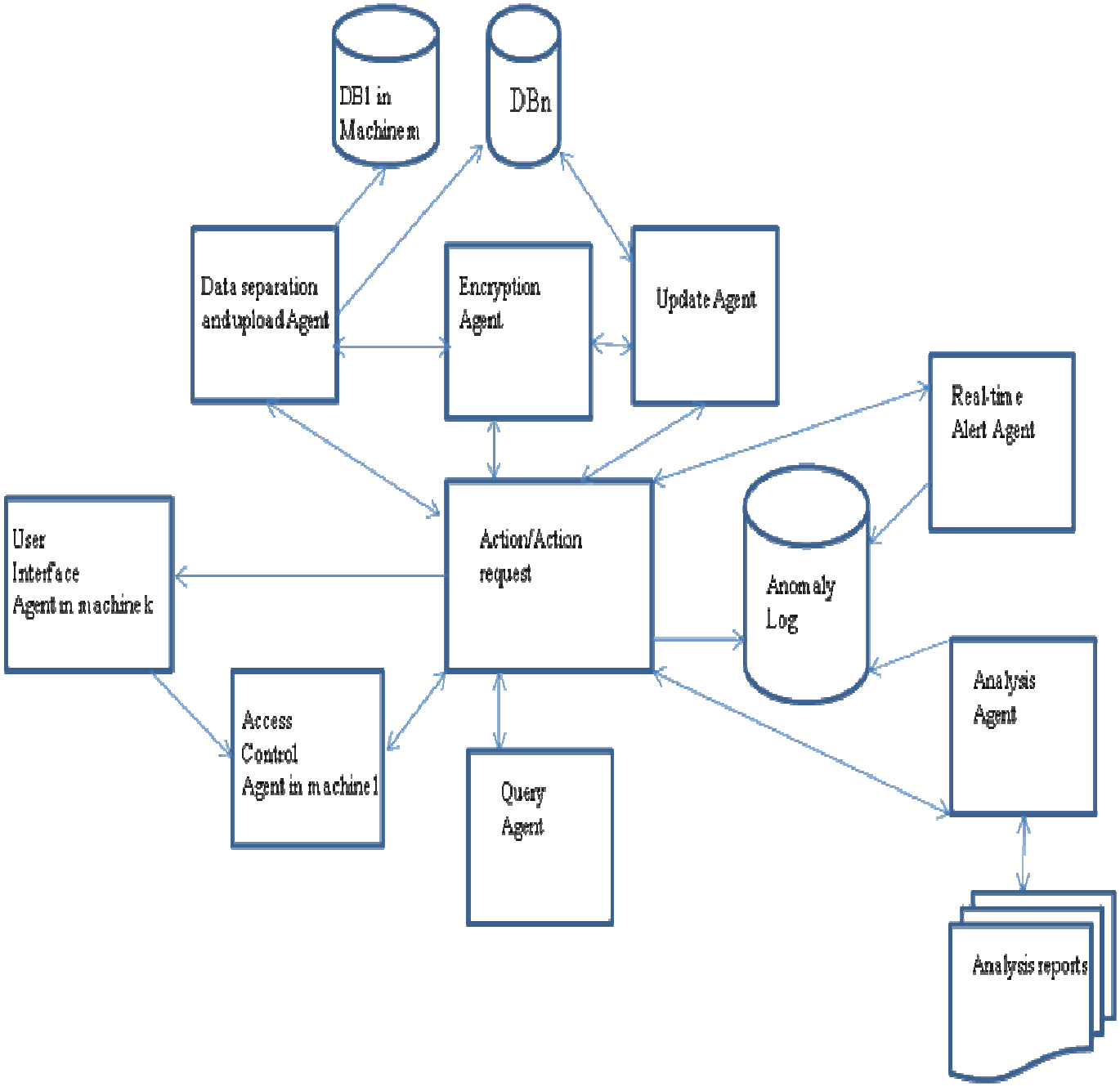


Figure 8: Architectural Design

4.3.2 Detailed Design

4.3.2.1 Block Interaction Diagram

Fig. 9 below shows Model Interaction Diagram

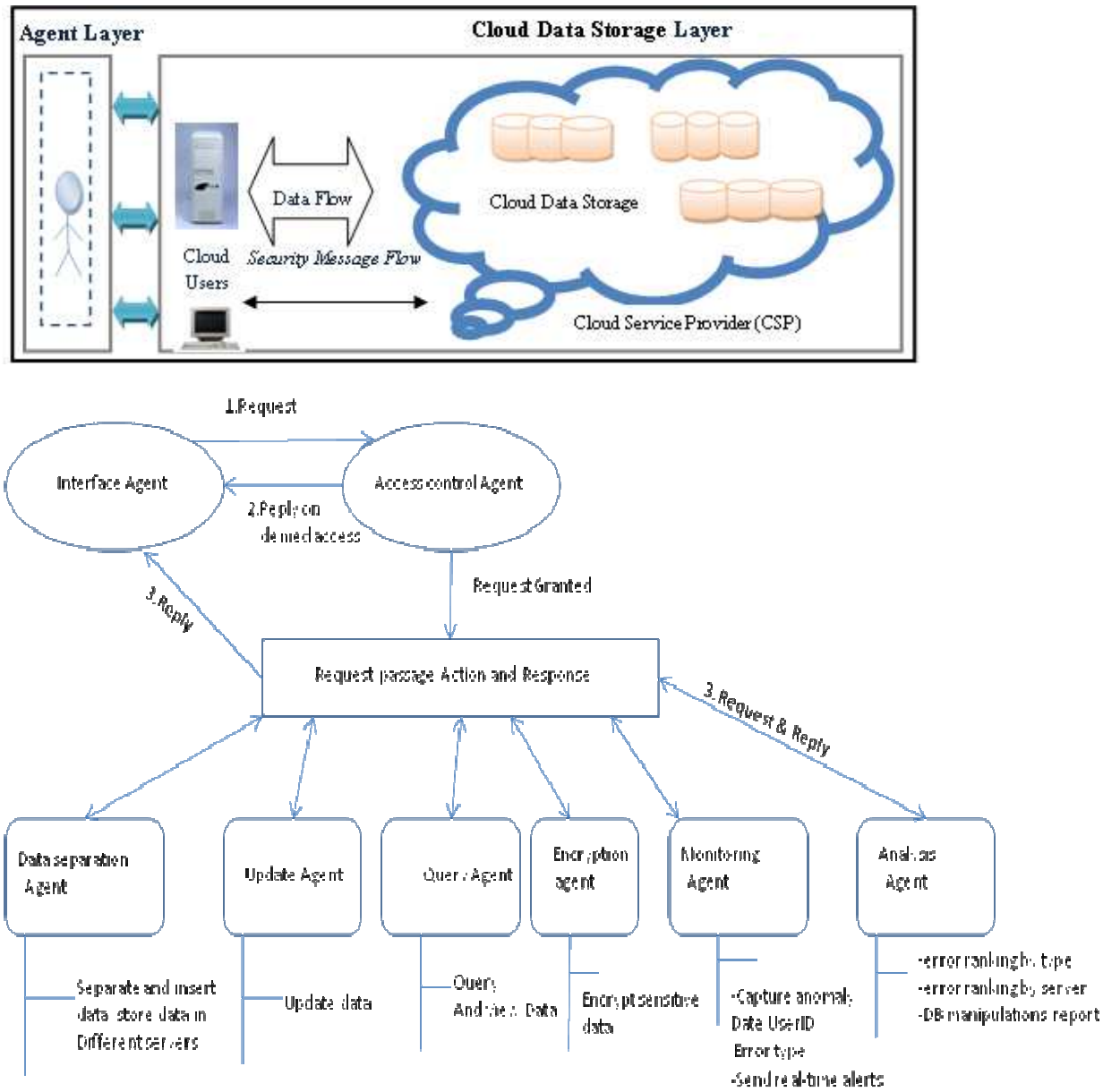


Figure 9: Model Interaction Diagram

4.3.2.2 Agents Use Case Diagram

Fig. 10 shows use case diagram for the model

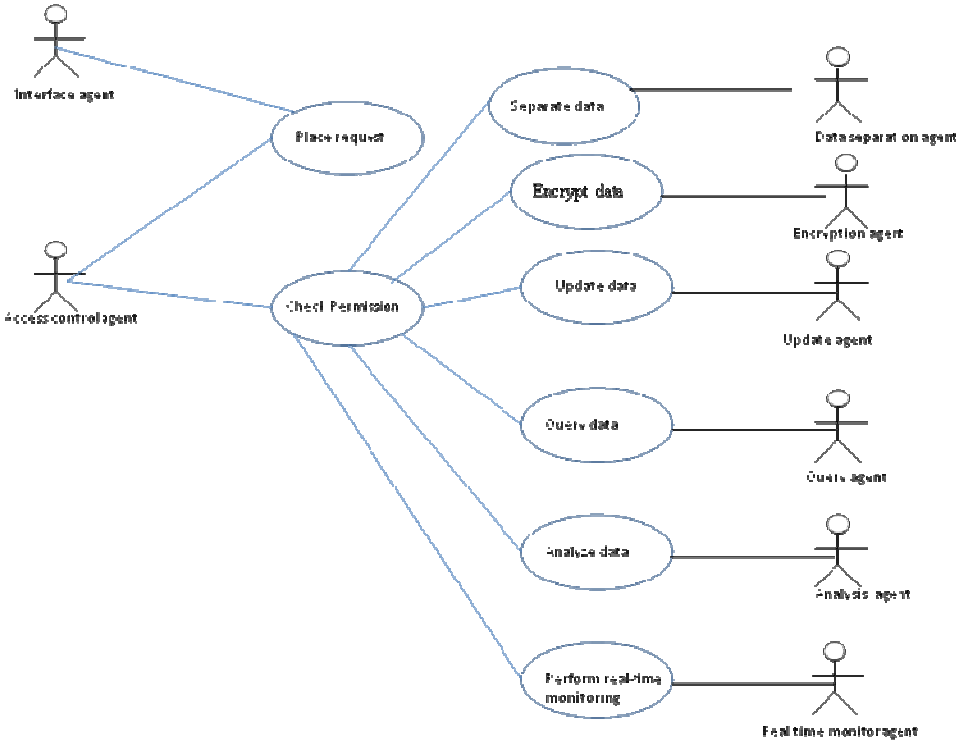


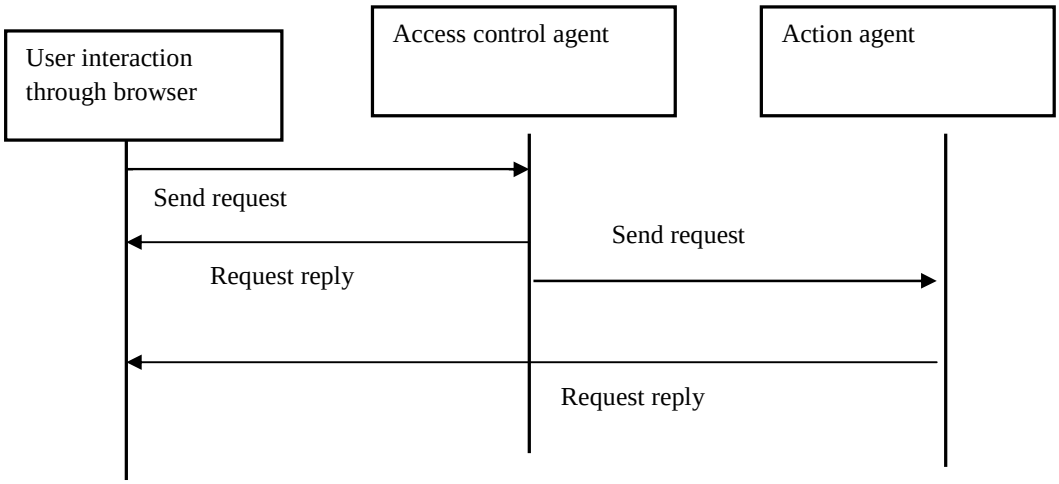
Figure 10: Use case diagram

4.3.2.3 Agents Communication Internals

i) User Interface Agent

This layer contains the application that allows users to interact with the system. Its primary role is to capture the user request and subject them to access control layer.

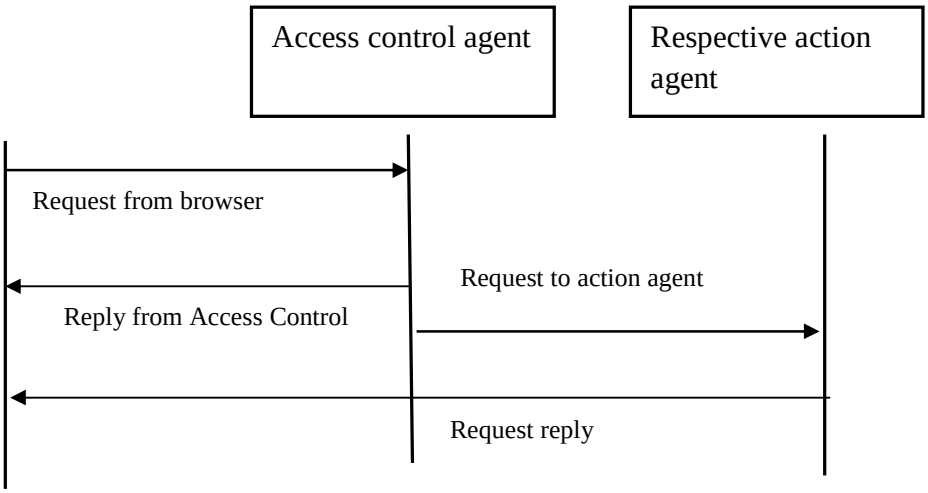
Interaction diagram for user interface



ii) Access Control Layer

This layer performs authentication and authorization then carries a given action

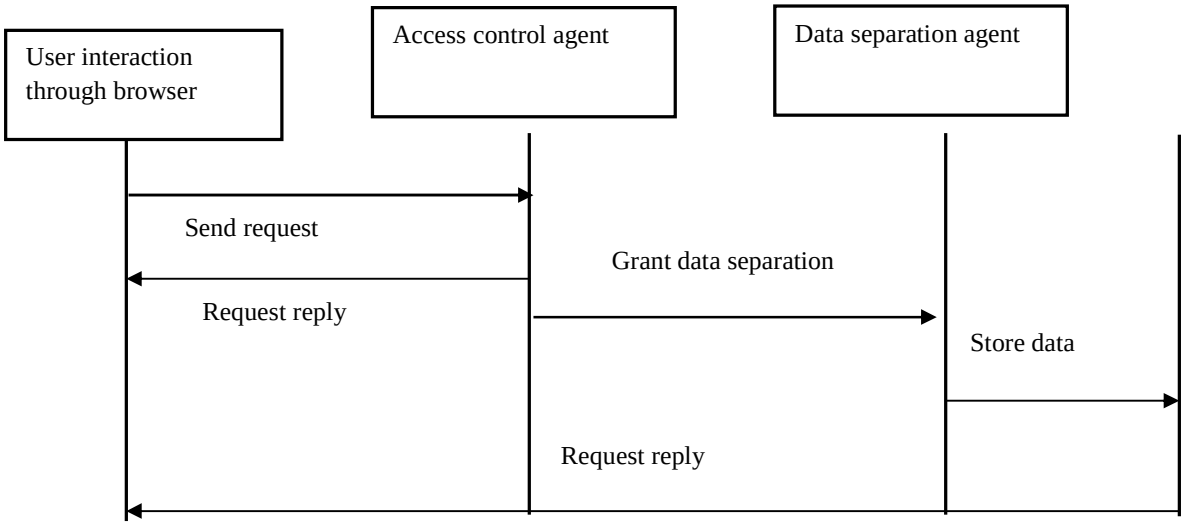
Access control interaction agent



iii) Data Separation Agent

The agent ensures database uploads or inserts are classified so as to store data appropriately. For migration of existing data, classification should be indicated on the schema i.e. Normal or sensitive data

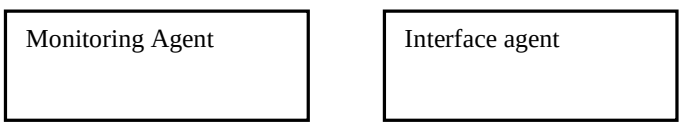
Data separation interaction agent

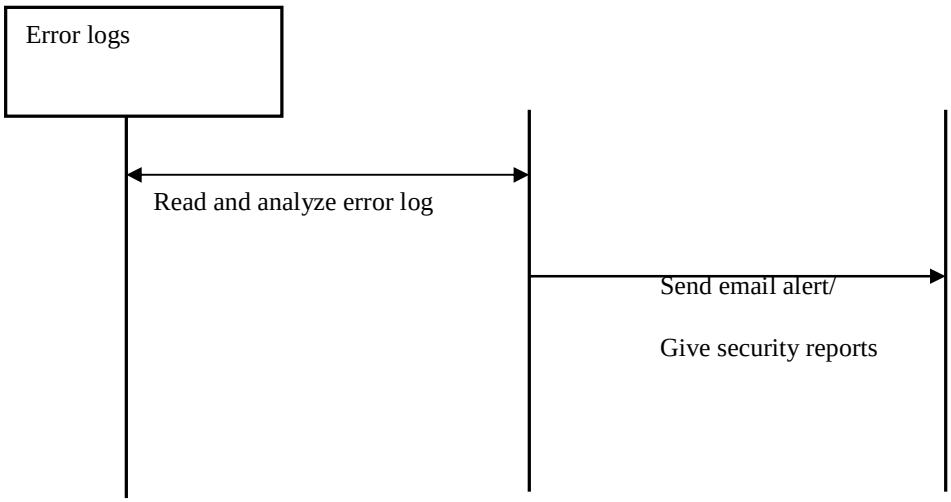


iv) Real-time monitor

Agent is responsible for relaying the anomalies on real-time basis. It sends the type of anomaly to the database administrator

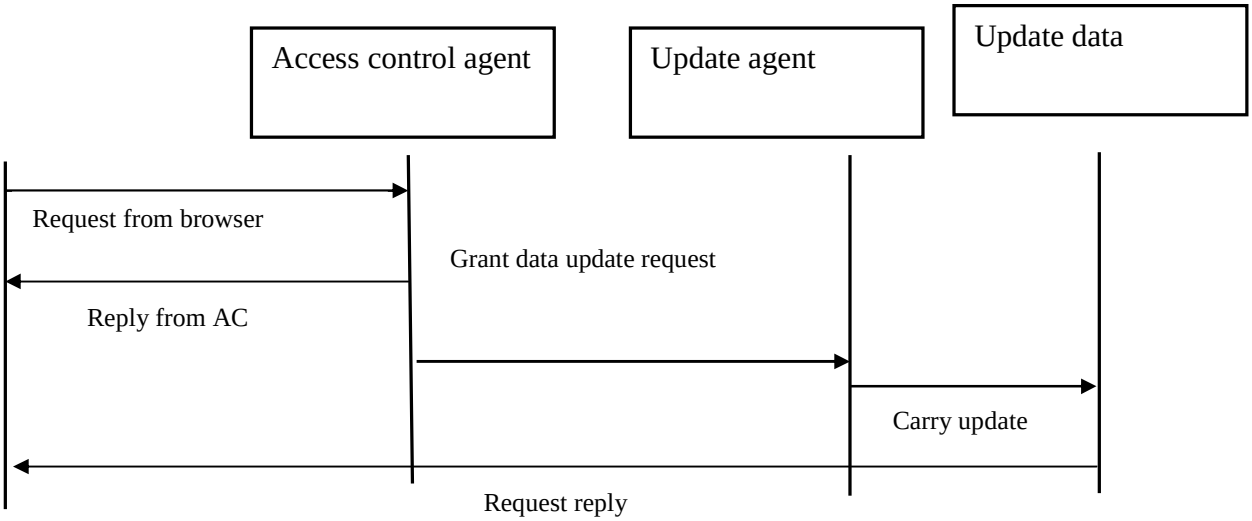
Interaction Diagram for Real time Alert Notification Agent





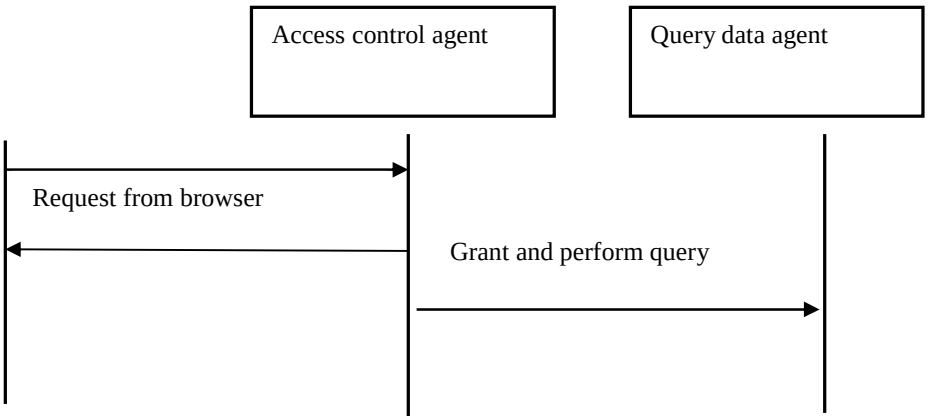
v) Update Agent

Performs database updates requests



vi) Query Agent

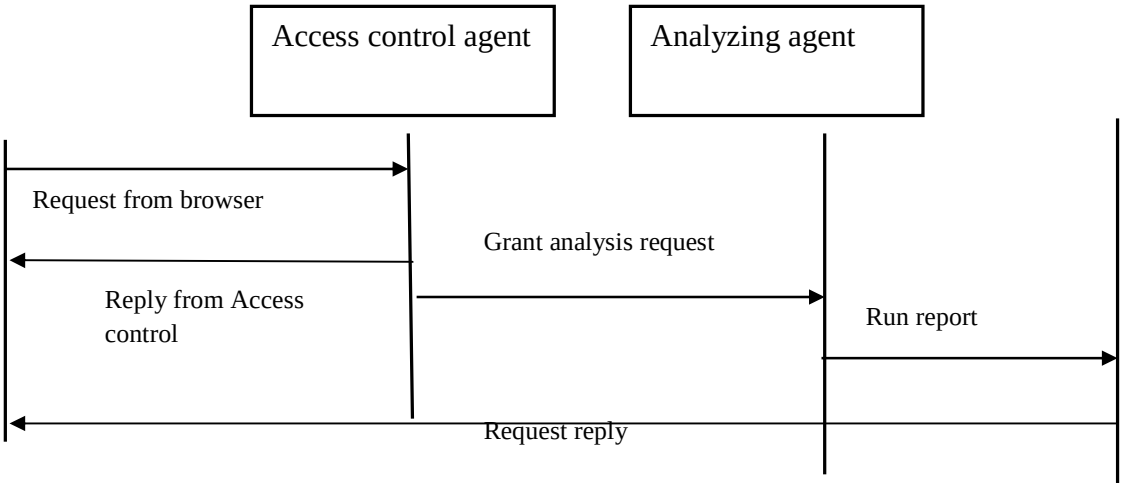
Agent that handles all the database queries



Reply from AC

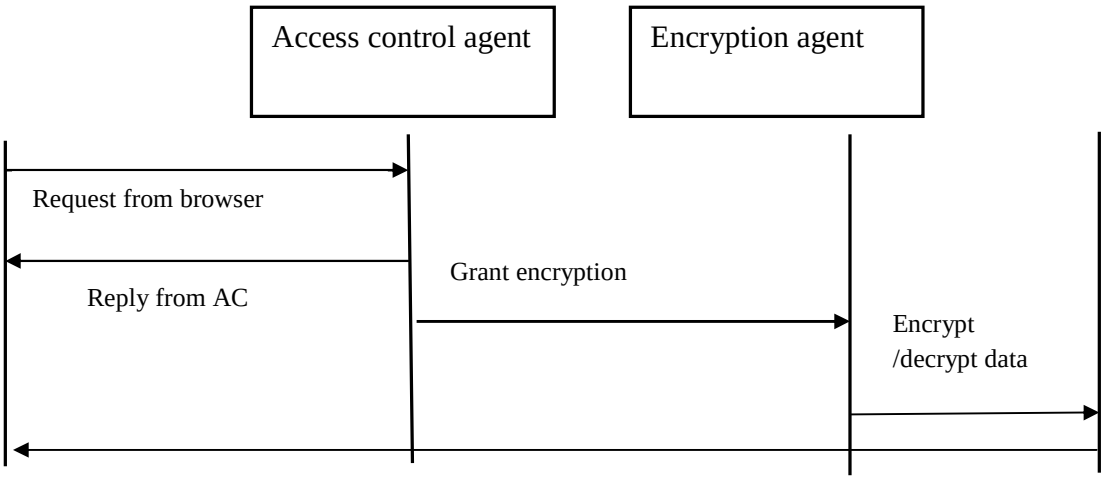
vii) Analysis Agent

Analyze the collected data in anomaly log database and performs vulnerability predictions



viii) Encryption agent

Performs encryption on sensitive data



4.3.2.4 Infrastructure Design

The model is composed of one host ma nes for demonstration purposes. A number of virtual machines can still be added depending on the number of storage servers. The host machine has Windows 7 operating system whereas the two oracle VM machines have windows XP operating software. Each of the machines has Mysql database and Wampserver which acts as web server. Figure 11 Shows the Oracle VM Setup.

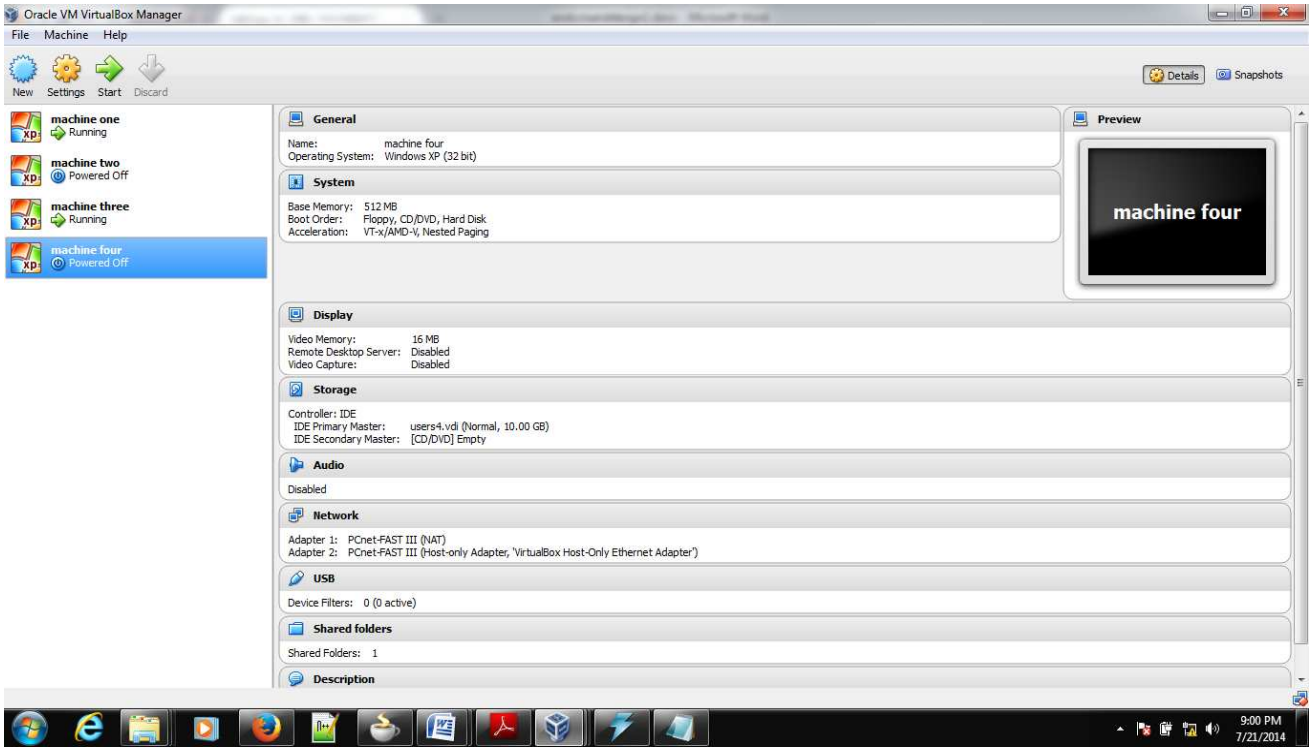


Figure 11: Oracle VM Setup

4.3.2.5 Database, Interface, Configuration, Main Menu Design

(Refer to Appendix 5 for database, Interface, Configuration and Main Menu Design)

4.4 System Implementation

The infrastructure was implemented by using Oracle VM Virtual Box and the application was implemented using Java Enterprise Edition (JEE) frame work with JADE, Oracle ADF running on Oracle Web logic server which acted as application server, Java Mail API utility, Gmail for SMTP as a mail server, MySQL 5.0.5 as a DBMS and Wamp Server as a web server. *(Refer to Appendix 6 for Model Code)*

4.5 Model Testing and Results

The model was tested using trial test cases that results to violations and non violations.

4.5.1 Sample Model Authorized Actions

i) Authorized separation of data to different servers

Figure 12 Shows login of user allowed carrying out record creation on different servers

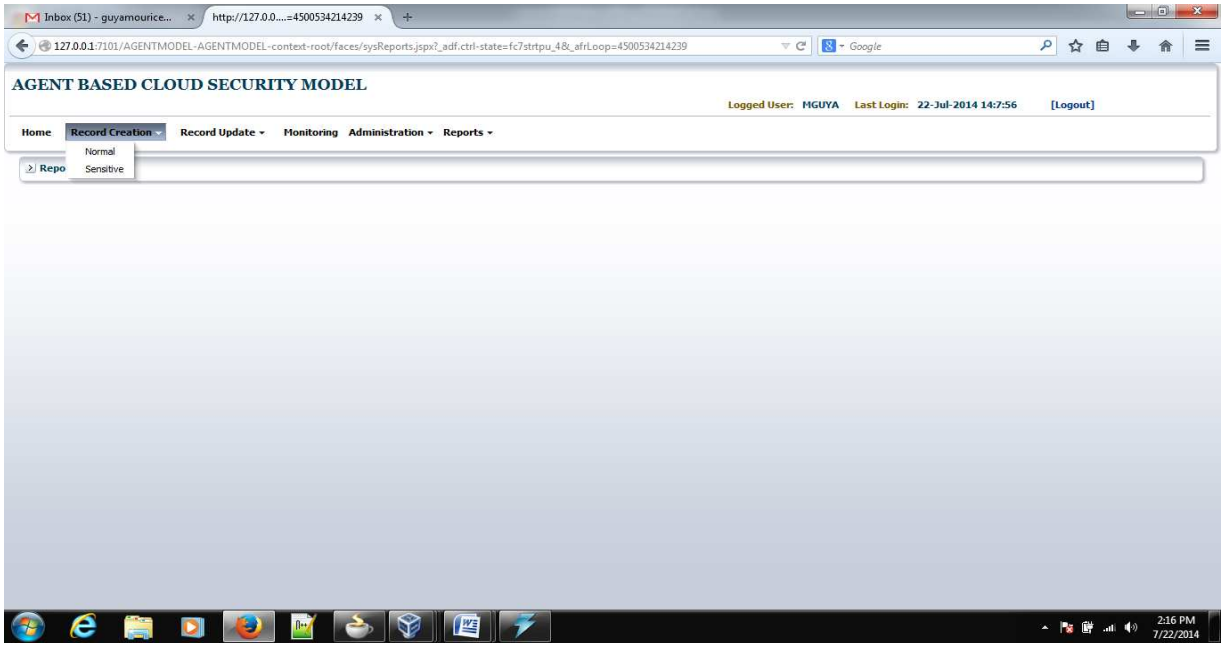


Figure 12: Authorized data separation screen

ii) Authorized update

Fig 13 Shows authorized updates on Payments server

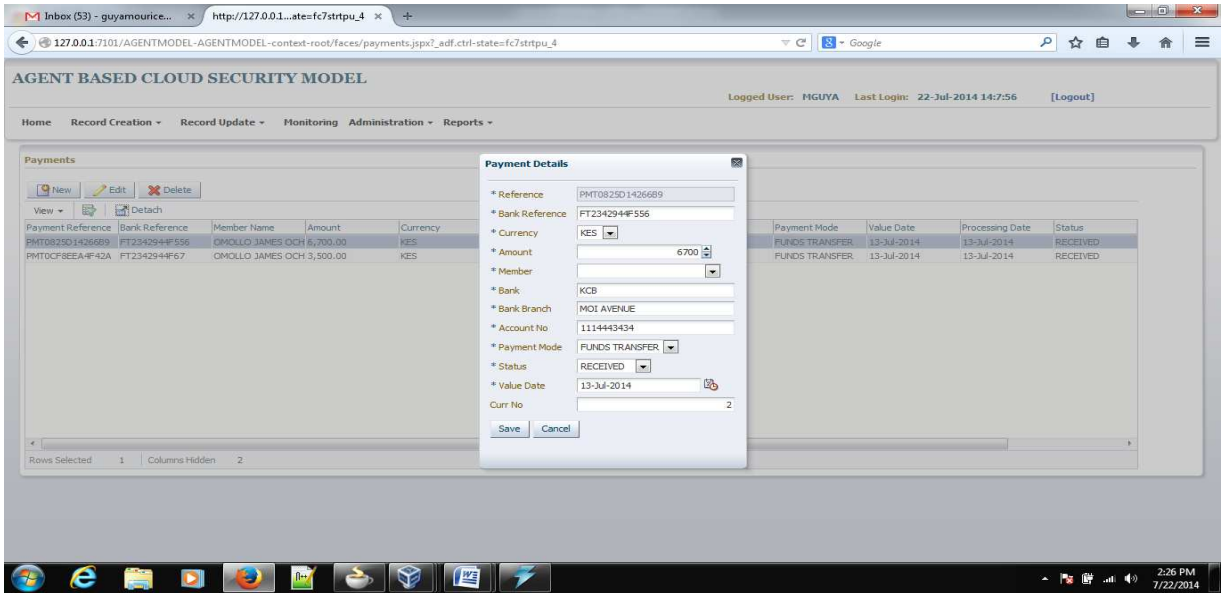


Figure 13: Authorized updates on Payments server

4.5.2 Sample Model Un-Authorized Actions and Reports

Figure 14 shows anonymous login error and Figure 15 Shows real time email alert

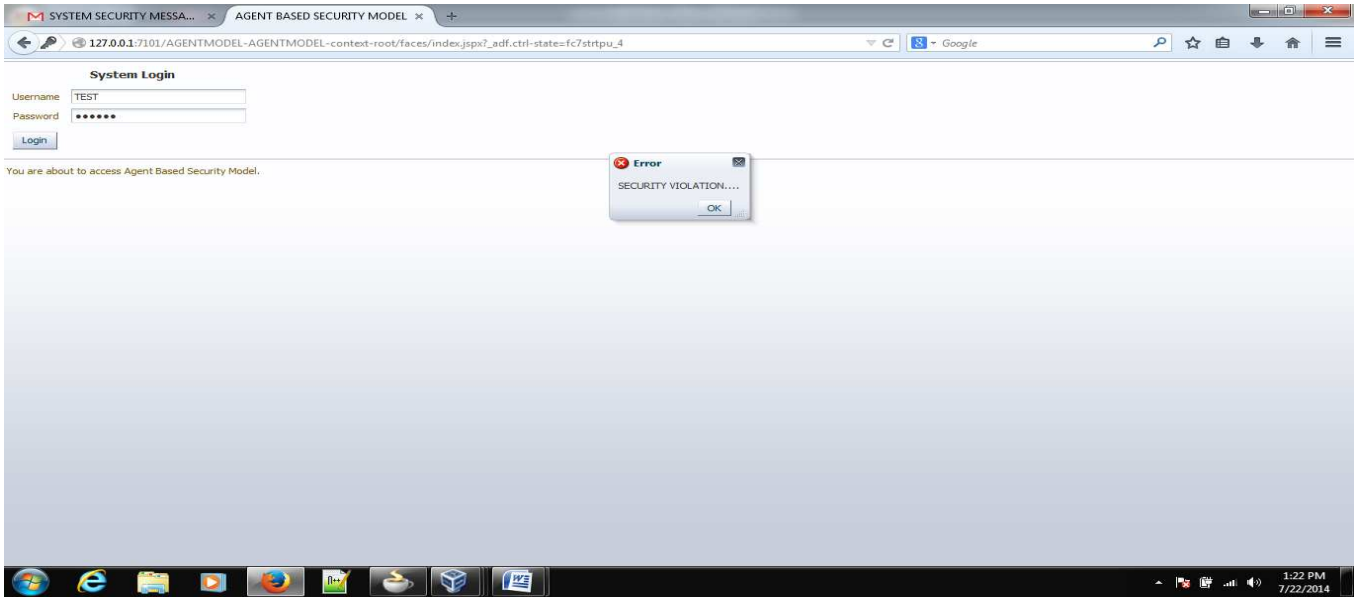


Figure 14: Anonymous login Error

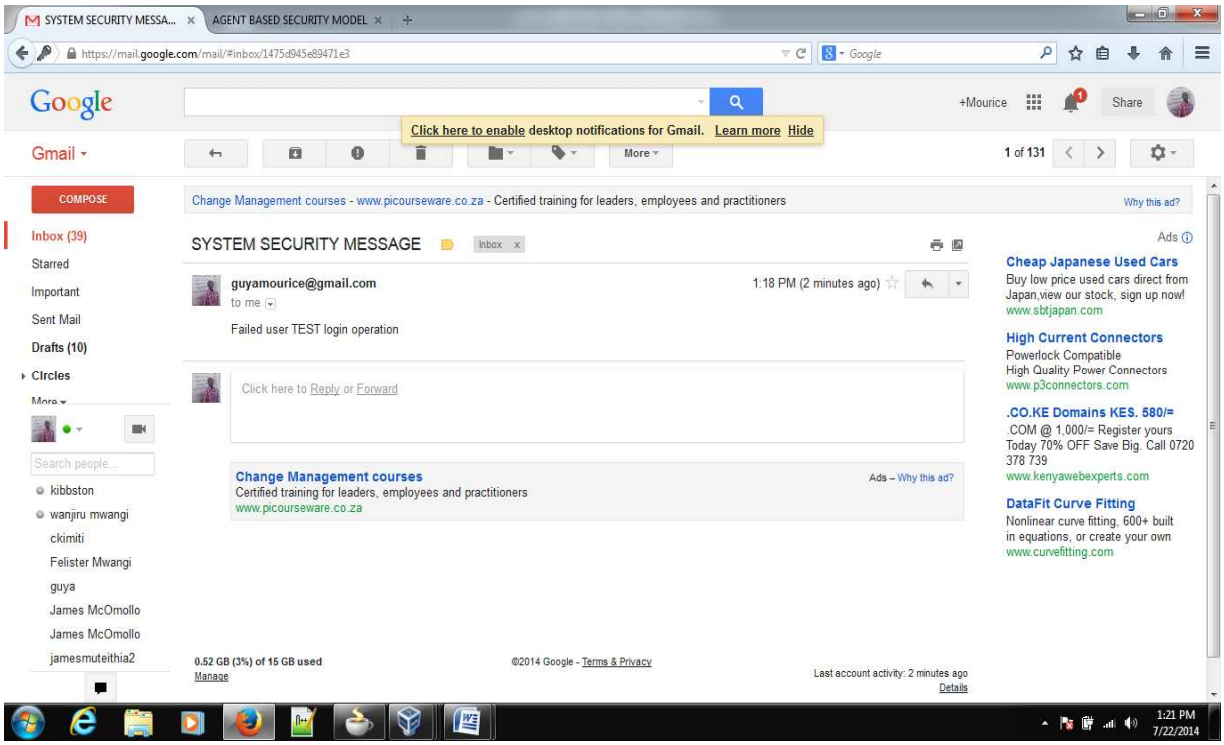


Figure 15: Anonymous real time email alert

Figure 16 Shows Inactivation of account upon 3 unsuccessful attempt

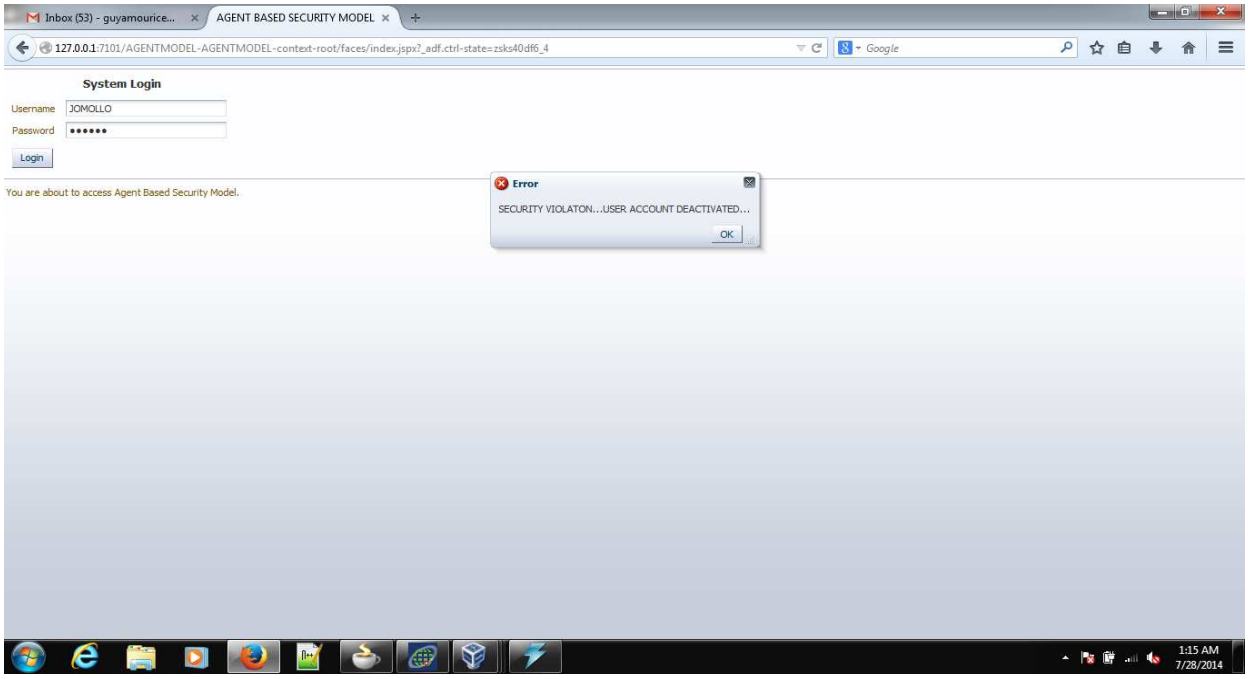


Figure 16: Account Inactivation

Fig 17. Shows insufficient privileges error and Fig 18. Shows real time email alert on insufficient privileges

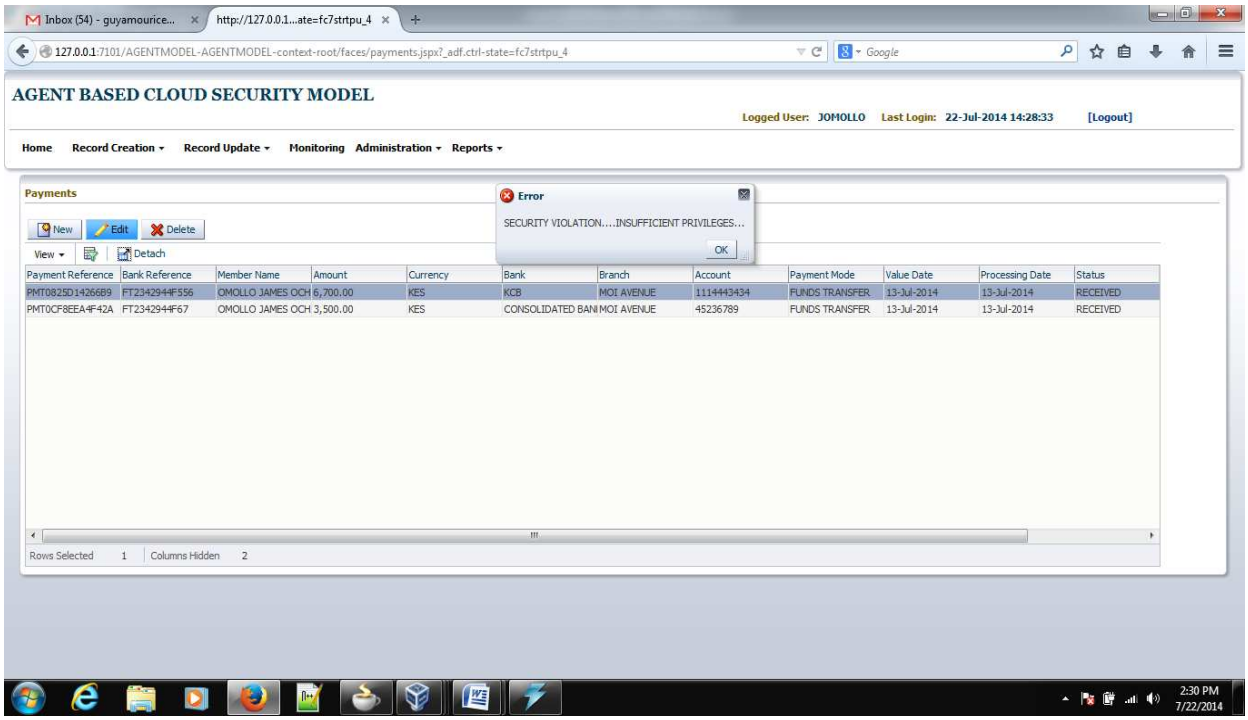


Figure 17: Insufficient privilleges error

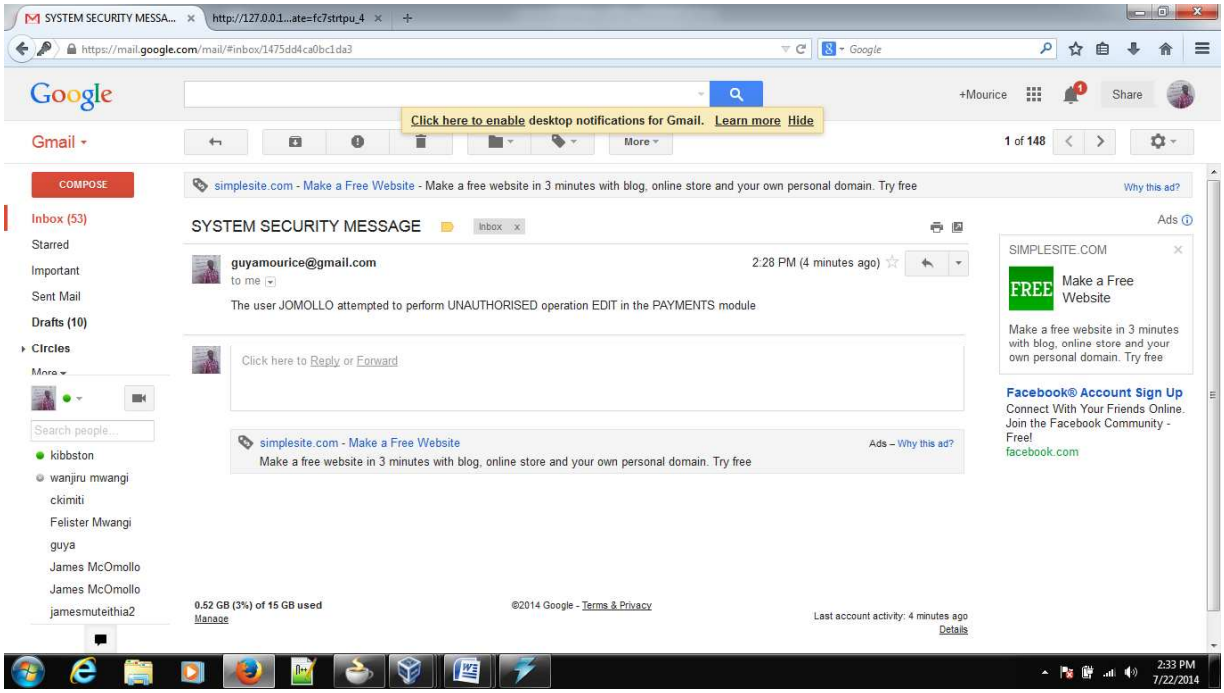


Figure 18: Insufficent privilleges email alert

Figure 19 Shows sample real time anomalies emails

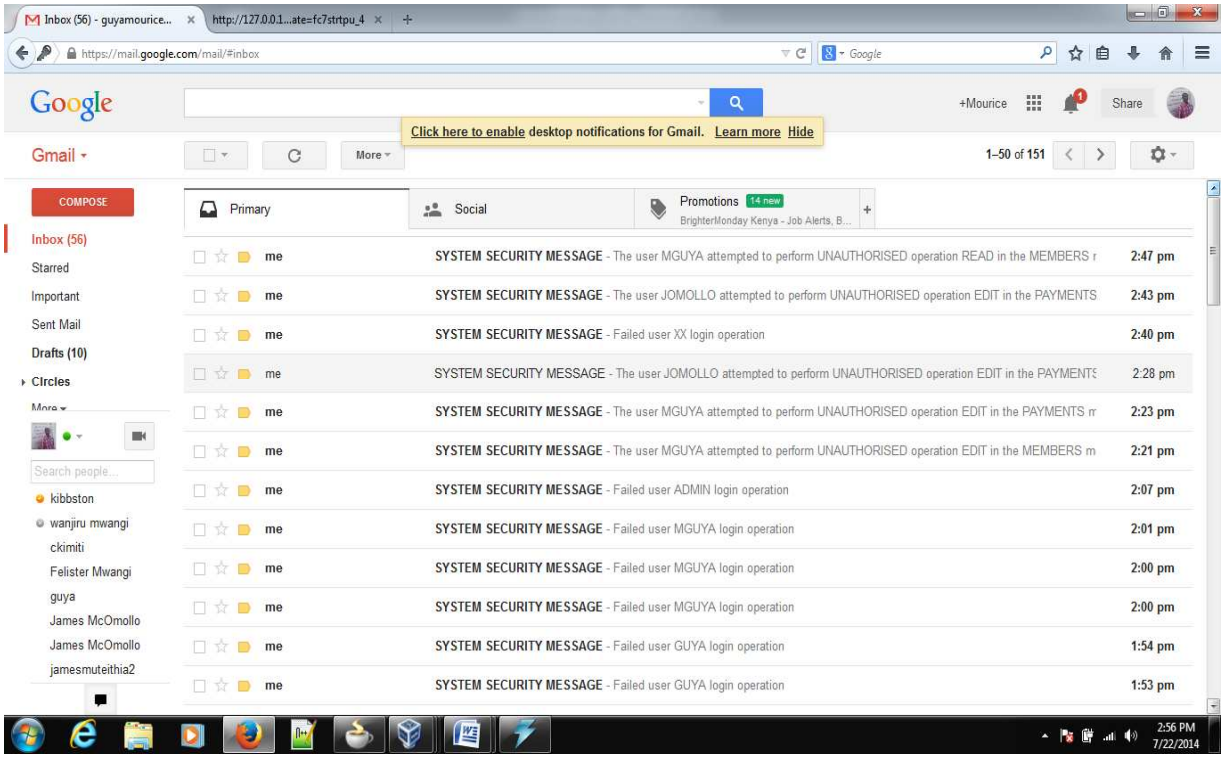


Figure 19: Sample anomalies Emails

Figure 20 Below shows sample system logs

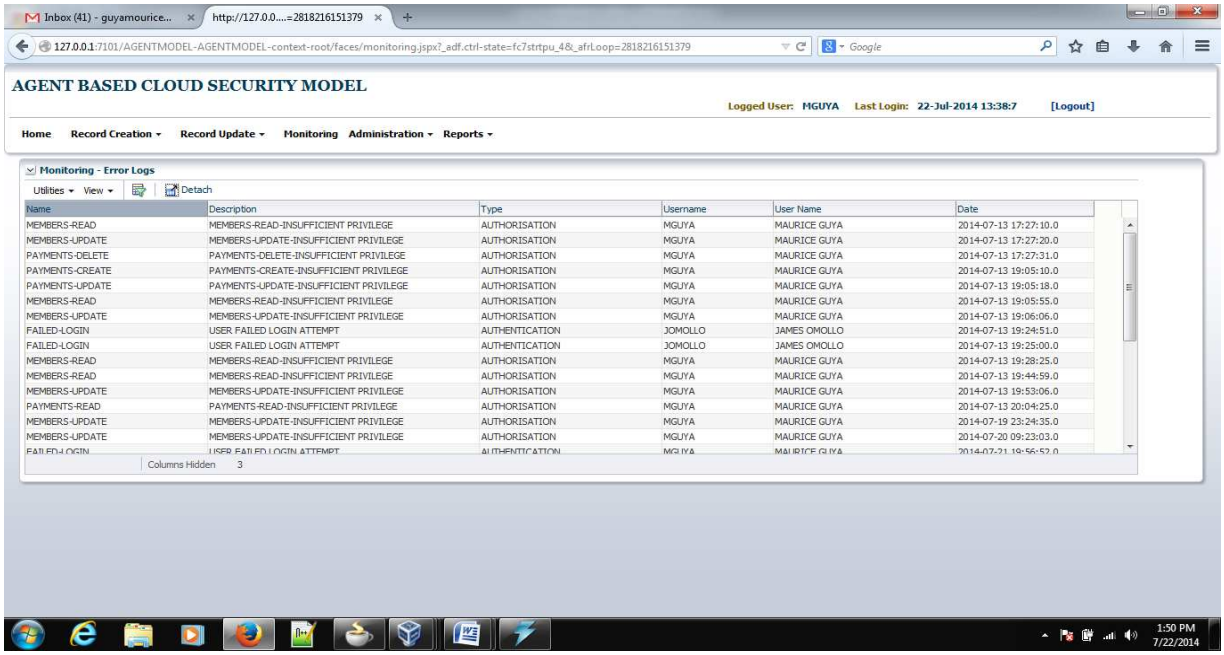


Figure 20: Sample System logs

Figure 21 Shows Servers Anomaly Ranking report

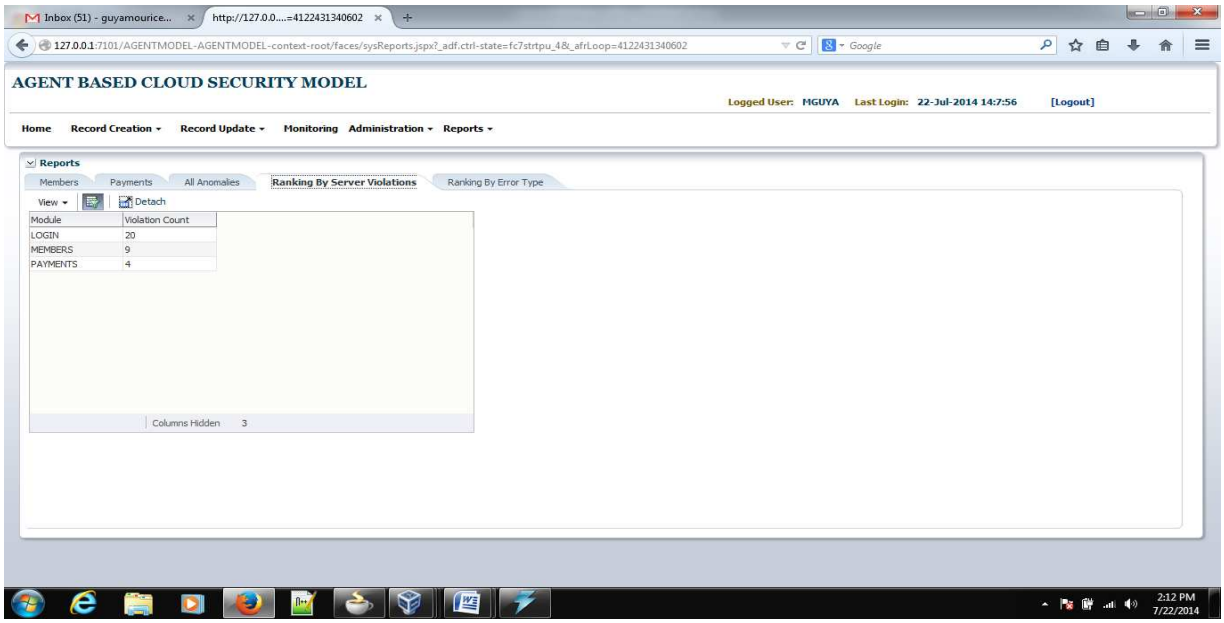


Figure 21 : Servers Anomalies Ranking report

Fig. 22 shows selective encryption

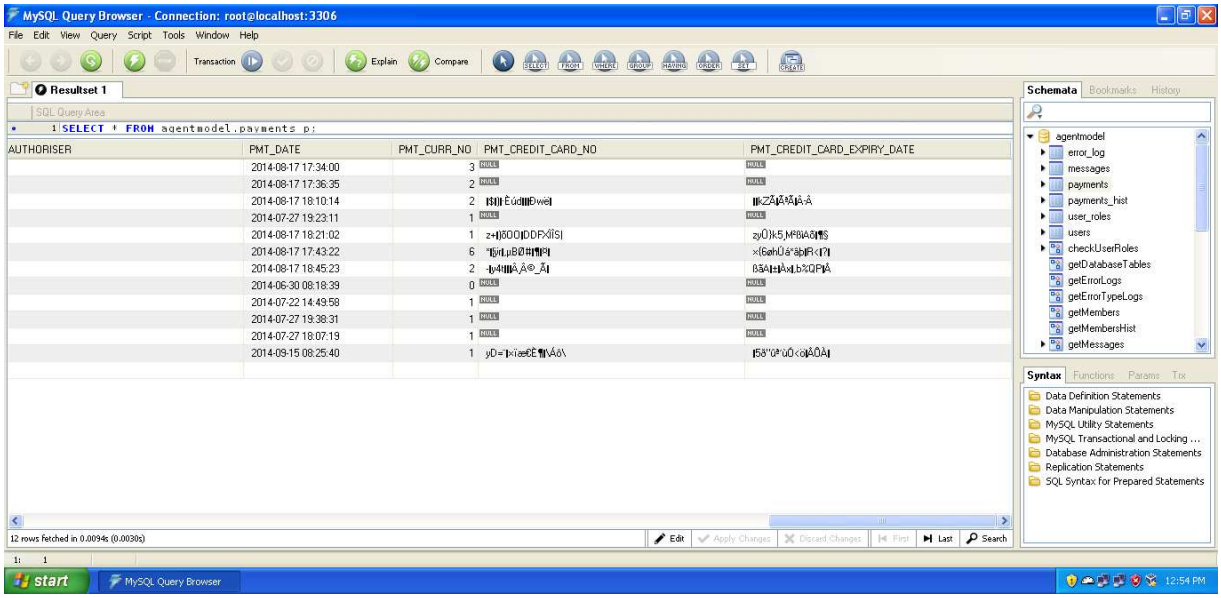


Figure 22: Sample selective encryption

4.6 Discussion of Results

4.6.1 Research Findings

Research results revealed security challenges faced by the stakeholders. Key findings on managers' revealed low strategic direction on cloud computing. 87.5% had not incorporated cloud in their organizational strategy and 78% did not know about cloud computing standards. 78% had security concern over cloud, 59.5 believed there was no control over cloud data. Findings on low awareness on standards i.e. 78% was almost in agreement with (Omwansa, Waema, Omwenga, 2014) in which had 75% as did not know about cloud computing standards. Low awareness was attributed to lack of exposure on benefits of cloud computing. The security challenges calls for real-time monitoring system, access control, selective encryption and data separation.

Findings on data custodians revealed 91.6% had security concerns, 100% believed encryption was the only protection mechanism, 70.8% allowed data migration to be done by the provider and 16.6% indicated monitoring as a way of ensuring control. Encryption has a number of performance degradation challenges thus other protection mechanisms are needed. Security concerns needed a combined security model and reliance on providers on data migration was attributed to lack of relevant expertise.

Findings on cloud providers revealed encryption as the only protection mechanism, no provision of real-monitoring systems, low compliance with industry standards and withholding of vital information from clients in regards to key management. Key highlight was low compliance with industry standards amongst the providers and lack of monitoring

systems. This pointed existence of high security vulnerabilities amongst the cloud service providers. The need for a model that performs real-time monitor, selective encryption and separate data storage so as to make data less important upon intrusion was necessary to curb the security challenges.

4.6.2 Model Findings

The model was able to perform the following: - Real-time monitoring of cloud environment, Data fragmentation across servers in different locations to enhance security, Encryption of only sensitive data so as to minimize encryption and decryption performance degradation, Enforcement of access control on all cloud objects and subjects, Production of security/vulnerability reports and database operations such as search, views, updates, deletions, insertions.

With real-time monitor, any data operations across different cloud service providers' storage are captured and this enhances control and transparency amongst the cloud customers. Data classification and separation allows data to be fragmented across different cloud service providers at different locations and this makes data incomplete upon successful intrusion. With Selective encryption, non-sensitive information doesn’t need to be encrypted and this minimizes the performance overheads associated with encryption and decryption. Vulnerability reports allow clients to rank different cloud service providers based on profiled security anomalies and also to rank anomalies by type across different cloud service providers.

4.6.3 Literature Review Security Challenges and Model solution

As captured in literature review, the two major techniques fronted for cloud security were access control, Encryption and SLA. Table 7 shows model security solution highlighting on techniques and user problems, main challenges and model solution.

Table 7: Model solutions

Techniques and Issues problems	**Challenges**	**Model solution and add ons**
i) Techniques		
Encryption	*-Brings performance degradation* Weis,Alves-Foss(2011);Chen(2012)Cryptography greatly affects database performance because each time a query is run, a large amount of data must be decrypted	*-Employs selective encryption* *-Provides data classification* Model offers data separation in which data is classified and stored at different locations. Part of data is encrypted based on sensitivity.
Access control	*-Intrusion* Intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system (Subashini and Kavitha, 2011).	*-Provides selective encryption* *-Provides real time monitoring* *-Provides data separation* Upon any successful intrusion by a hacker, the information is incomplete
SLA	*SLA Violations*	*-Provides Real time monitor*
ii) User Security Challenges		
Reduced control over data		*Access control and real-time monitoring*
Un-authorized access		*Access control, Data separation and Encryption*
SLA Violations		*Real-time Monitoring*
Encryption performance degradation		*Data separation and selective encryption*
		Multi-agents Properties
		Negotiation: *user agent ,access control, data separation, encryption, updates, Queries*
		Autonomy: *monitoring, access control*
		Communication: *all agents*
		Reactive: *Inactivation after invalid logins, email alerts*
		Proactive: *prevent inactive accounts from logging in*
		Intelligence : *Security Analysis reports*

4.6.4 Model Solution and Literature Review

The model has provided a combined solution on implementation of data classification and separation proposal(Chen,2012),Access control(Yuefa et al,2009;Darsi et al,2013), encryption(Darsi et al,2013) , use of agents in cloud security(Talib,2010) , usage of agents to search, filter, query and update the massive volumes of data that are stored (Talia, 2011) with addition of real time data monitoring.

4.6.5 Model Results

As shown in section 4.5 Model Testing and Results, the model is able to monitor and perform real time alert notifications, performs data classification and store data in different servers, encrypt only sensitive data ,provide security analysis reports and performs data manipulation operations such as:- search ,updates, deletion and insertions.

CHAPTER FIVE

CONCLUSION

5.1 Achievements

The research objective of exploration of existing security techniques, finding security challenges amongst cloud stakeholders and system objective of development and testing of agent-based security model for database applications was achieved. The combination of major research works namely data classification and separation proposal (Chen,2012), Access control (Yuefa et al, 2009; Darsi et al, 2013), use of agents in cloud security (Talib,2010;Talia), Encryption (Darsi et al, 2013) with addition of real time data monitoring is a major achievement by this model. A number of cloud users expressed their security fears in regards to cloud applications more so on privacy, reduced control and lack of transparency in handling of their data by the cloud providers. This security fear has been effectively handled by real-time data monitoring that sends violated user actions to client database administrators.

The model developed has explicitly shown that it is practically possible to use agents to classify data, store data in different locations with different cloud providers, encrypt only sensitive data and perform data manipulation and monitoring. The data separation and selective encryption reduces volume of data to be encrypted thereby decreasing encryption and decryption performance degradation issue.

From the model tests, the following results were obtained:- Real-time monitoring on cloud database applications, Data classification and storage at different locations ,Selective encryption of data, Access control, Security Analysis reports, Database manipulations allowing Search, Updates, Inserts and Deletions

5.2 Limitations

This model is purposely designed for organizational based database applications but can be extended to cover other cloud applications storage services such as dropbox, icloud, google drive. The model majorly brings selective encryption, real-time events monitoring, data classification and storage separation and will be integrated with other existing mechanisms

such as identity management systems. Changes to existing conventional databases are unavoidable as different databases calls for reorganization and classification before being moved to cloud. There is cost incurred during data separation and mapping at runtime however this cost is negligible since there is no conversion needed and fragmentation is already a feature inherent in distributed systems, this cost is lesser than the cost of encrypting and decrypting all the data in database systems.

5.3 Research Contributions

The research focused on combining different facets of security approaches for cloud applications so as to increase cloud usage by users and organizations as security has been a major hindrance in cloud uptake, this project demonstrates that agent framework can be used to combine various security approaches so as to provide multifaceted security in cloud computing arena. The model brings in data classification, selective encryption as well as real-time data monitoring in cloud environment. Data classification reduces the volume of data for encryption so as to minimize encryption performance degradation and selective encryption minimizes performance overhead associated with encryption and decryption. This model shows that agents framework can be used to combine the various security approaches.

5.4 Future work

Future work will involve inclusion of agent-based federated identity management comprising of Service providers, Identity providers and Users (Rasim & Fargana, 2013) and Use of mobile agents across network(Ali,Abdullah,Kazar,2013).

REFERENCES

[1] USA. Computer Security Division (2011) *The NIST definition of cloud computing.* Gaithersburg: NIST (SP800-145) [Special Publication]

[2] Mather, T., Kumaraswam, S., Latif, S. (2008) *Cloud security and Privacy*. O'REILLY

[3] Ritesh, G., Chatur, P., Swati.G. (2012)Cloud Computing and Security Models: A survey. *International Journal of Engineering Science and Innovative Technology* [Online] 1(2/November). P.1-6. Available from: http://www.ijesit.com [Accessed: 02 February 2014]

[4]Pearson, S. (2012) Security and Trust in Cloud Computing. HP Laboratories

[5] El-khameesy, N., Rahman, H. (2012) A proposed model for Enhancing Data Storage Security in Cloud Computing Systems. *Journal of Emerging Trends in Computing and Information Sciences* [Online] 3(6/June).p.2. Available from: http://www.cisjournal.org[Accessed:02 Jan 2014]

[6] Subashini, S. & Kavitha, V. (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and computer Applications* [Online], 34(July).p.3.Available from:www.elsevier.com/locate/jnca

[7] Kandukuri, B., Paturi, R., & Rakshit, A. (2009) *Cloud security issues. International Conference on Services Computing:* April 2009. Pune, India.

[8] Choudhary V. (2007) *Software as a service: implications for investment in software development. Proceedings of 40th Hawaii International conference on system sciences*

[9] Weis, J., & Alves-Foss, J. (2011).Securing Database as a Service.*IEEE Security and Privacy*. vol. 9, no. 6, p.49-55,

[10] Chen, D., & Zhao H. (2012) *Data Security and Privacy Protection Issues in Cloud Computing*. *Proceedings of 2012 International Conference on Computer Science and Electronics Engineering*.Shenyang, China, Available from: http://xa.yimg.com/kq/groups/2584474/417972861/name/NDU-1.pdf

[11] Balding, C. (2008). Is your machine Image vulnerable to SSH Spoofing Attacks.Cloud security. Available from: http://cloudsecurity.org/2008/07/14/is-your-amazon-machine-image-vulnerable-to-sshspoofing-attacks [Accessed: 03-Jan-2014]

[12] Mitchell, I., & Alcock, J. (2010) *The White Book of Cloud Security.* [Online] London: Fujitsu Services Ltd. Available from:http://www.fujitsu.com/es/Images/WBOC-2-Security.pdf.[Accessed:14th Jan 2014].

[13] Omwansa, T., Waema, T., & Omwenga, B. (2014) Cloud Computing in Kenya: A 2013 Baseline Survey. [Online]Available from http://www.c4dlab.ac.ke/wp-content/uploads/2014/04/

CC-study-report-April-2014.pdf [Accessed: 21st May 2014].

[14] ITU (2012) Cloud Computing in Africa: Situation and Perspectives. Telecommunications DevelopmentSector.[Online]Availablefrom:http://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique- e.pdf [Accessed: 21st May 2014].

[15] Ovum. (2012) Enterprise considerations for cloud computing [Online] Available from:

http://www.cio.co.ke/news/main-stories/enterprise-considerations-for-cloud-computing.[Accessed:23 May 2014]

[16] Kituku, M. (2012) *Adoption of Cloud Computing in Kenya by Firms listed in the Nairobi Stock Exchange*. Unpublished.[Online]Available from: http://erepository.uonbi.ac.ke/handle/11295/13578[Accessed: 23rd May 2014]

[17] IARA. (2014) *The 5th International Conference on Cloud Computing, GRIDs and Virtualization.*Venice, Italy.May25-29, 2014.Availablefrom: http://www.iaria.org/conferences2014/CLOUDCOMPUTING14.html.[Accessed:13th Feb 2014]

[18] CSA. (2014) *Secure Cloud 2014.Amsterdam,* Netherlands.April1-2, and 2014.Available from: https: /cloudsecurityalliance.org/events/securecloud2014. [Accessed: 13th Feb 2014]

[19] *CSA. (2014)Summit 2014. RSA, SAN FRANCISCO, USA.Feb 24 2014.Available from*

*h*ttps://cloudsecurityalliance.org/events/csa-summit-2014 [Accessed: 13th Feb 2014]

[20] CCSW. (2013)*The ACM Cloud Computing Security Workshop*.Berlin, Germany.8th Nov 2013.Available from: **http://www.digitalpiglet.org/nsac/ccsw13/**[Accessed: 13th Feb 2014]

[21] SCC. (2013)*International Workshop on Secure Cloud Computing*. Xian, China.Sep 9-11, 2013.Available from: http://crises-deim.urv.cat/scc2013/ [Accessed: 13th Feb 2014]

[22] Darsi,M.,Suresh,K., & Jayakumar,S.(2012) A new approach for providing the data security and secure data transfer in cloud computing .*International journal of computer trends and*

technology. [Online]4. (5/May).Available from: http://www.ijcttjournal.org/Volume4/issue-5/IJCTT-V4I5P47.pdf [Accesed: 18 Feb 2014]

[23] Mani, M., Shah, K., & Gunda, M. (2013) Enabling Secure Database as a Service using fully Homomorphic Encryption: Challenges and Opportunities. P.1

[24] Mulero, V. (2009) *Privacy and Anonymization for very large datasets.*Barcelona, Spain. November2009.Availablefrom: tp://dl.acm.org/citation.cfm?id=1646333

[25]Yuefa, D., Bo, W., Yaqiang, G., Quan, Z., & Chaojing, T. (2009) *Data Security Model for Cloud Computing. Proceedings of 2009 International Workshop on Information Security and Application* (IWISA 2009), Qingdao, China, November 21-22, 2009, Available from: www.academypublisher.com/proc/iwisa09/papers/iwisa09p141.pdf [Accessed: 22 Feb 2014].

[26] Talia, D. (2009) Cloud Computing and Software Agents: Towards Cloud Intelligent. [Online] Available from: http://ceur-ws.org/Vol-741/INV02_Talia.pdf [Accessed: 22 Feb 2014].

[27] Talib, A. (2010) Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature Review: Computer and Information Science. [Online] 3(4/November).Available from: www.ccsenet.org/cis [Accessed: 23 Feb 2014)

[28] Rasim, A., & Fargana, A. (2013) *Identity Management Based Security Architecture of Cloud Multi-Agent Systems.6th International Information Security & Cryptology Conference*, Turkey. Available from:www.iscturkey.org/iscold/ISCTURKEY2013/files/paper11.pdf *[Accessed: 23 Feb* 2014)

[29] Padgham, L., & Winikoff, M.Australia. (2014) The *Prometheus Methodology* [Online] Available from: http://goanna.cs.rmit.edu.au/~linpa/Papers/bookchB.pdf

APPENDICES

Appendix 1: Different sets of Questionnaires

Appendix 2: Analysis of Cloud Service Providers Questionnaires

Appendix 3: Analysis of Managers' Questionnaires

Appendix 4: Analysis of DBAs, System Administrators, System security Administrators Questionnaires

Appendix 5: Database, Interface, Configuration, Main Menu Design

Appendix 6: Sample Model Code

Appendix 1: Questionnaires

i) Cloud providers Questionnaires

Your Name _____ Company _____

QUESTION	ANSWER
How do you safeguard data in the cloud(for database applications)	
Who manages encryption keys	
Where are encryption keys kept	
How do you safeguard data leakage on shared resources	
Which industry standard do you comply with	
Are mechanisms for identification, authorization and key mngt	
How is your data backup mechanism for cloud data	
How do you destroy data when it's no longer required	
List FIVE of your cloud customer clients	

ii)Managers Questionnaires Cloud Computing Questionnaire for Managers/Directors

Your Name _____ Company Name_____

QUESTION	ANSWER
Have you ever used Cloud computing services ?	Yes ☐ No ☐
Do you intend to use cloud computing services ?	Yes ☐ No ☐
What benefit do you get/expect to get from Cloud computing?	
What are your concerns about cloud computing?	
Has cloud computing been formerly incorporated into your Organization strategy?	
Which operation in your Organization have you taken to cloud or are you planning to take to cloud?	
Who owns your data in the cloud and who has the right to use it?	
How do you curb SLA(Service Level Agreement) Violations	
How do you provide governance and assurance over the services migrated to the cloud?	
What continuity procedures are available in the event of failure of cloud service?	
Has the cloud provider availed audit and assurance information? e.g procedure documentation ,Certifications e.g ISO 27001,PCI,COBIT,BS 25999,Logging and monitoring information	
Tick if you have used any the following	Dropbox ☐ Salesforce CRM ☐ Office 365 ☐ Googledocs ☐ Socious Microsoft Dynamics ☐ Oracle Cloud ☐

iii)Data Custodian Questionnaires Cloud Computing Questionnaire for DBA/SA/Security Administrators

Your Name _____ Company Name_____

NOTE: For check boxes, double click to check

QUESTION	ANSWER
Have you ever used Cloud computing services	Yes ☐ No ☐
Do you intend to use cloud computing services	Yes ☐ No ☐
Which cloud computing service are you already using or which you intend to use	
What benefit do you get/expect to get from cloud computing	
What are your concerns about cloud computing in regards to moving your DB to the cloud	
How do/will you ensure there is no intrusion to your data	
How will/do you ensure your cloud data is secure?	
How will/do you ensure you have control over your DB on the cloud	
How will/did you migrate your data to the cloud? (Consider that you can migrate the data yourself or use the cloud provider to migrate the data for you)	
Tick if you have used any the following	Dropbox ☐ Salesforce CRM ☐ Office 365 ☐ Googledocs ☐ Socious Microsoft Dynamics ☐ Oracle Cloud ☐

Appendix 2: Analysis of Cloud Service Providers Questionnaires

The companies names have been represented with letters for confidentiality purposes

RESEARCH QUESTION	**RESPONDENTS**			
	B	C	A	**COMMENTS**
How do you safeguard data	Encryption and authentication	Encryption	Encryption	Only encryption being used
Is there any data protection mechanism apart from encryption	No	No	No	No other protection mechanism
Are there monitoring systems	No	No	No	No monitoring
Industry standard	ISO 27001	None(CSA not std)	None (Not specific,ITIL and ISO)	Recommended ISO 27017(Purely for cloud),27002,27000,27001, PCI DSS,SSAE 16,HIPAA,Sarbanes-Oxley
Are users in control	Access control	Access control	SLA	Access control minus monitoring functionality
Who manages encryption keys	Customer	Provider	Client	Not advisable for provider to manage encryption keys
Where are encryption keys kept	Customer decides	Data Centre	Customer defines and keep	Not advisable for provider to keep keys
How do you safeguard data leakage	In SaaS ,each customer has virtual environment, In IaaS VM is mapped to independent VRF	Identity provisioning	VLANS,OSFW,DMZ	A more efficient form is fine grained multi-tenancy, where all resources are shared, except that customer data and access capabilities are segregated within the application, K-anonymity,DLP,Data Leak as a service
How do you handle media disposal /clearance of client data upon contract termination? is degaussing performed?	Information purged on customer request	Clean sweep	Depends on ownership and kind of data	Degaussing needed to remove residual data

Appendix 3: Analysis of Managers Questionnaires

QUESTION	Total	No response	Don't Know	Ambiguous/Wrong	Average	Correct/Answer given	
What benefit do you get/anticipate to get from Cloud computing?	35	3	4			28	-Cost effective,shared resources,scalability,Elasticity, -Ease of Access,High data processing speed,Storage,Flexibility
What are your concerns about cloud computing?	35	3	4	3 Costly		25	-Security(privacy, redundancy, data intrusion, unauthorized access, access controls, data ownership, monitoring)
Has cloud computing been formerly incorporated into your Organization strategy?	35	3	4			NO 28	YES
Which operation in your Organization have you taken/plan to take to cloud?	35	3	4			28	
How will/do you ensure operational transparency/control is enforced over your cloud data?	35	3	19	4 -Training users -backups		9 -Access control -monitoring -SLA	Real time monitor, External Audits
Who owns your data in the cloud ?	35	3	6	20 -Service provider -my self		6 ourselves	Client owns the data ,CSP and users are granted access as per SLA
How will/do you provide governance and assurance over the services migrated to the cloud?	35	3	23	2 Supervisor to check		7 SLA	-Internal Audit on cloud services -CSP to disclose external audits based on standards e.g ISO 27017, 27002,27000,27001,27018,27031 PCI DSS,SSAE 16
Do you have comprehensive disaster recovery plan for cloud services?	35	3	22	4 -we will plan for it		6	
Has the cloud provider availed audit and assurance information? e.g procedure documentation ,Certifications e.g ISO 27001,PCI,COBIT,BS 25999,Logging and monitoring information	35	3	26	1 -Not yet used		5	

Appendix 4: Analysis of Data custodian Questionnaires

QUESTION	Total	No response	Don't Know	Ambiguous/Wrong	Average	Correct	
What benefit do you get/anticipate to get from Cloud computing?	24					24	-Cost effective -shared resources -scalability -elasticity -Ease of Access -High data processing speed -Storage -Flexibility
What are your concerns about cloud computing?	24				Lack of general Awarenes s 2	24	-Security(privacy, redundancy, data intrusion, unauthorized access, access controls, data ownership, monitoring)
How will/do you ensure cloud data is secure?	24					-Encryption(18) -Encription and access control(6)	-Encryption -Access Control -Data separation -monitoring
How will/do you enforce disaster recovery plan?	24					24 SLA (11) Assurance(13)	-SLA -Transparency -Assurance on restorations -Backups mechanisms -Replication mechanisms
How will/do you ensure you have control of your DB on the cloud?	24					-Access control (19) -SLA & Access control (5)	-Access control -SLA -Monitoring
How will/did you migrate data to the cloud ? (Consider that you can migrate the data yourself or allow provider to migrate for you)	24			Provider 17		7	-Migration tool managed by client

APPENDIX 5: Data base, Interface, Configuration, Main menu Design

1) Data base Design

i) User Accounts Table

Field Name	***Type***	***Key***
USR_CODE	*INT(10)*	*Primary*
USR_NAME	*VARCHAR(45)*	
USR_PASSWORD	*VARCHAR(45)*	
USR_STATUS	*VARCHAR(45)*	
USR_LOGIN_ATTEMPTS	*INT(10)*	

iii) PAYMENTS TABLE

PMT_CODE	*VARCHAR(45)*	*Primary*
PMT_REF	*VARCHAR(45*	
PMT_AMOUNT	*VARCHAR(45)*	
PMT_BMR_NO	*VARCHAR(45)*	
PMT_BANK	*VARCHAR(45)*	
PMT_BRANCH	*VARCHAR(45)*	
PMT_ACCOUNT	*VARCHAR(45)*	
PMT_MODE	*VARCHAR(45)*	
PMT_STATUS	*VARCHAR(45)*	
PMT_DATE	*DATETIME*	
PMT_CURR_NO	*INT(10)*	

„„v) USER ROLES TABLE

Field Name	***Type***	***Key***
ROLE_ID	*INT(10)*	*Primary*
ROLE_USR_CODE	*INT(10)*	
ROLE_TABLE_NAME	*VARCHAR(45)*	
ROLE_CREATE	*VARCHAR(45)*	
ROLE_READ	*VARCHAR(45)*	
ROLE_UPDATE	*VARCHAR(45)*	
ROLE_DELETE	*VARCHAR(45)*	
ROLE_DATE	*TIMESTAMP*	
ROLE_STATUS	*VARCHAR(45)*	

vii) Anomalies/Error log Classification

Name		*Type*
Insert		*Insert*
Update		*Update*
Delete		*Delete*
Attempted login without account		
Valid account attempting unauthorized permission		
Valid account with wrong password		

ii) BIO Table

Field Name	***Type***	***Key***
MBR_CODE	*INT(10)*	*Primary*
MBR_SURNAME	*VARCHAR(45)*	
MBR_OTHER_NAMES	*VARCHAR(45)*	
MBR_EMAIL	*VARCHAR(45)*	
MBR_PHONE	*VARCHAR(45)*	
MBR_DOB	*DATETIME*	
MBR_STATUS	*VARCHAR(45)*	
MBR_NOK_NAME	*VARCHAR(45)*	
MBR_CUR_NO	*INT(10)*	

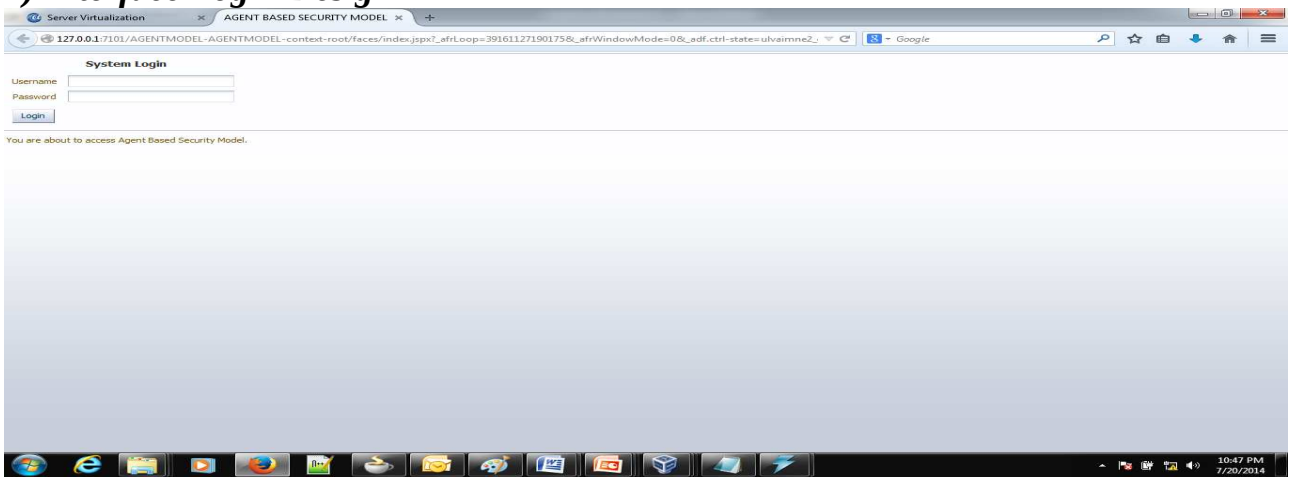
iv) ERROR_LOG TABLE

Field Name	***Type***	***Key***
LOG_ID	*INT(10)*	*Primary*
LOG_NAME	*VARCHAR(45)*	
LOG_DESC	*VARCHAR(45)*	
LOG_STATUS	*VARCHAR(45)*	
LOG_USER	*VARCHAR(45)*	
LOG_DATE	*TIMESTAMP*	
LOG_TYPE	*VARCHAR(45)*	
LOG_MODULE	*VARCHAR(45)*	

vi) MESSAGES TABLE

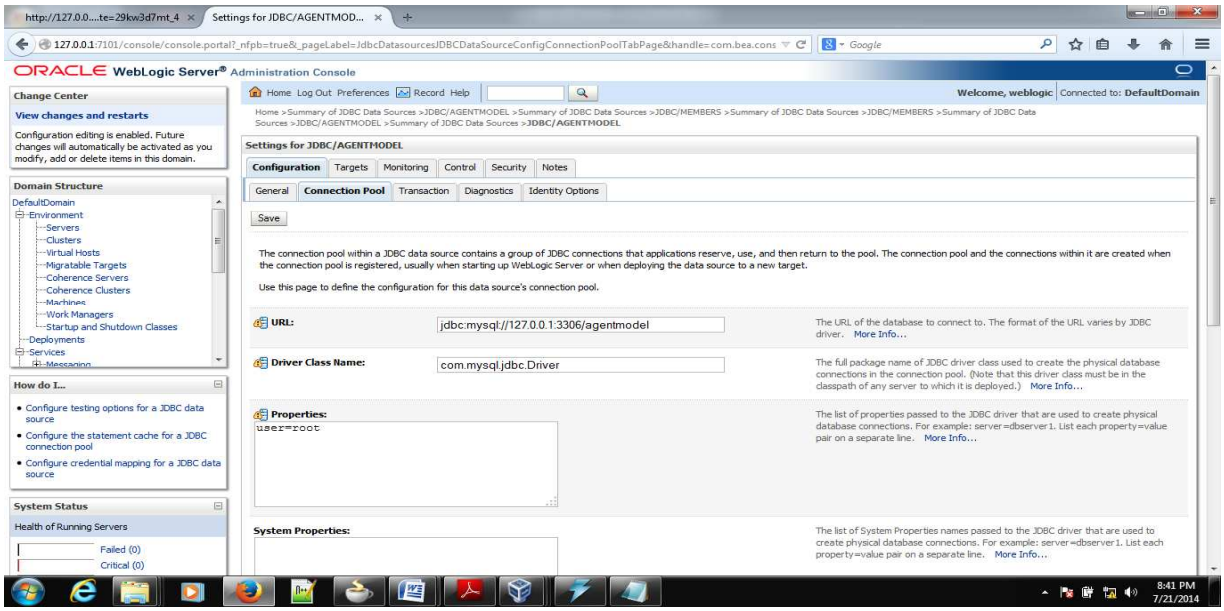
Field Name	***Type***	***Key***
MSG_CODE	*INT(10)*	*Primary*
MSG_TYPE	*VARCHAR(45)*	
MSG_DESCRIPTION	*LONGTEXT*	
MSG_SENDER	*VARCHAR(45)*	
MSG_RECEIVER	*VARCHAR(45)*	
MSG_STATUS	*VARCHAR(45)*	
MSG_DATE	*DATETIME*	
MSG_USR_CODE	*INT(10)*	

2) Interface Login Design

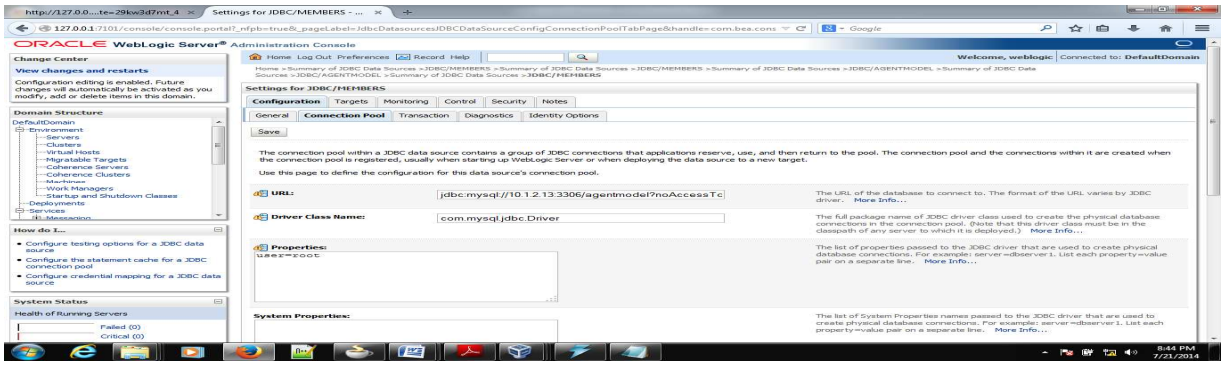


3) Data Sources Configuration

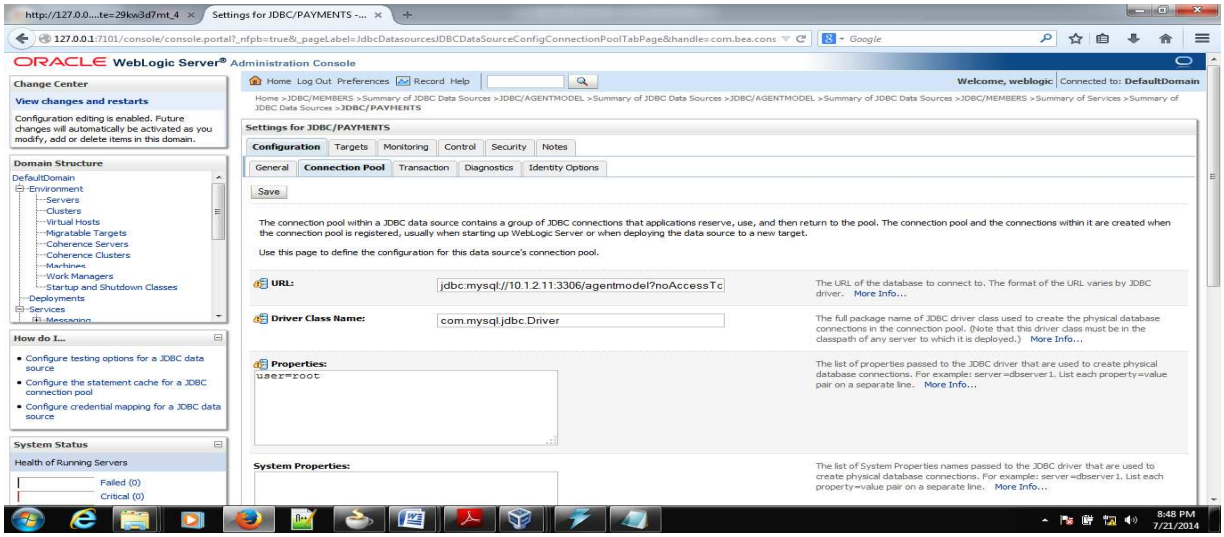
i) IP Address for host machine (127.0.0.1)



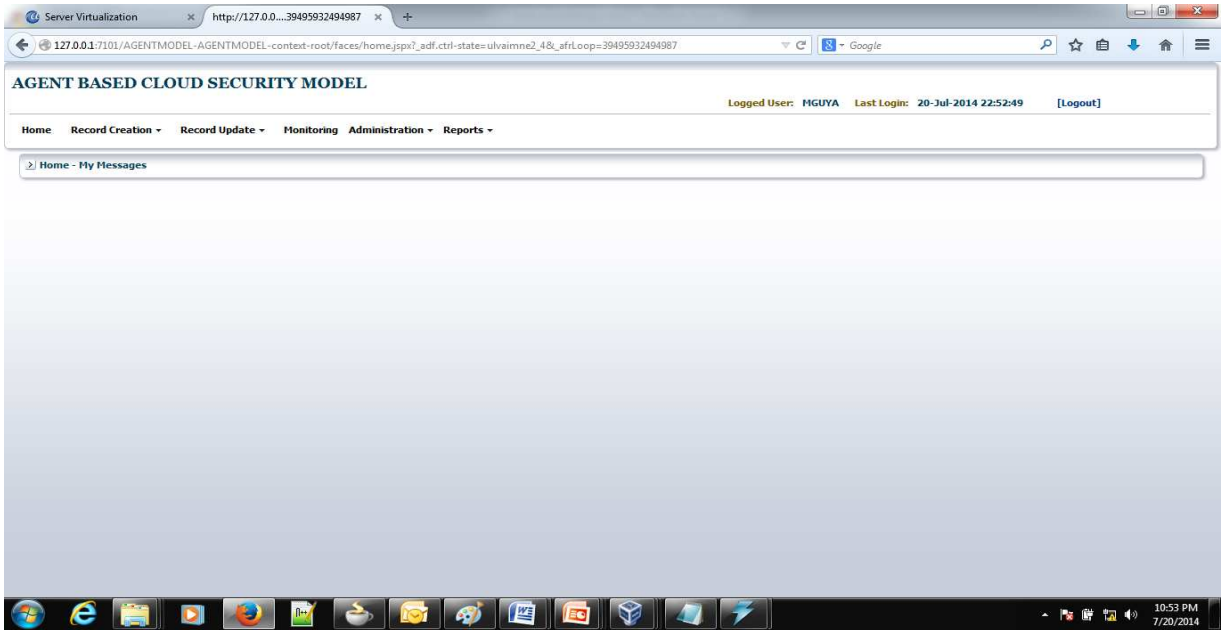
ii) IP address for virtual machine BIO Information Server (10.1.2.13)



IP address for Virtual Machine Payments Information Server (10.1.2.11)



4) Model Main Menu Design Screen



Appendix 6: Sample Model Code

Interface Agent

```
<?xml version='1.0' encoding='UTF-8'?>

<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page" version="2.1"

 xmlns:f="http://java.sun.com/jsf/core"          xmlns:h="http://java.sun.com/jsf/html"    xmlns:af="http://xmlns.oracle.com/adf/faces/rich">

  <jsp:directive.page contentType="text/html;charset=UTF-8"/>  <f:view>     <af:document id="d1" title="AGENT BASED SECURITY MODEL">      <af:form id="f1" defaultCommand="cb1">    <h:panelGrid columns="1" id="pg3" style="text-align:center;">

       </h:panelGrid>   <af:separator id="s1"/>        <h:panelGrid columns="1" id="pg5" style="text-align:center;">

         <af:outputLabel value="System Login" id="ol4"  inlineStyle="font-weight:bold; font-size:small; color:inherit;"/>

         <h:panelGrid columns="1" id="pg1">   <h:panelGrid columns="3" id="pg7">  <af:outputLabel value="Username" id="ol1"/>

            <af:inputText label="Label 1" id="it1" simple="true"    binding="#{Authenticate.loginUsername}"/>

            <af:outputLabel id="ol5"/>  <af:outputLabel value="Password" id="ol2"/>

            <af:inputText label="Label 2" id="it2" secret="true" simple="true"  binding="#{Authenticate.loginPassword}"/>

          </h:panelGrid>  <h:panelGrid columns="1" id="pg2">   <af:commandButton text="Login" id="cb1" action="#{Authenticate.login}"/>   </h:panelGrid>       </h:panelGrid>    </h:panelGrid>    <af:separator id="s2"/>

       <h:panelGrid columns="1" id="pg4">    <af:outputLabel value="You are about to access Agent Based Security Model."

                    id="ol3"/>  </h:panelGrid>  </af:form>   </af:document>  </f:view></jsp:root>
```

// Access Control Agent

```
package com.agent.auth; public class Authenticate {

      }    HttpSession session = (HttpSession)FacesContext.getCurrentInstance().getExternalContext().getSession(false);

   private String loggedUser;    private Date loginDate;

  /* This agent handles user login authentication against set Usernane and Password. It also check whether the user attempting to log in  is a registered or anonymous user. In case of anonymous user, security violation error message is raise and an alert sent to the system admin.

   * It also deactivate a user account on three failed login attempts. All violations are also logged for reporting.

   * A successful login lands the user on home page (home.jspx) ans sets the UserCode,username and logged in date sessions.

   */    public String login() {        String userNameVal =    GlobalCC.checkNullValues(loginUsername.getValue());

      String passwordVal =    GlobalCC.checkNullValues(loginPassword.getValue());    if (userNameVal == null || passwordVal == null) { GlobalCC.RaiseErrorMessage("Enter username and password");

          return null;  }        DBConnector datahandler = null; datahandler = new DBConnector();  Connection conn;  conn = datahandler.getDBConnection();  String value = null; String anonymous = null;  BigDecimal userCode = null;  CallableStatement cst = null;

      String query = "{ CALL userAuthenticate(?,?,?,?,?,?) }";   try {  cst = conn.prepareCall(query);  cst.setString(1, userNameVal); cst.setString(2, passwordVal); cst.registerOutParameter(3, Types.NUMERIC); cst.registerOutParameter(4, Types.VARCHAR); cst.registerOutParameter(5, Types.VARCHAR); cst.registerOutParameter(6, Types.NUMERIC);  cst.execute();  userCode = cst.getBigDecimal(3); value = cst.getString(4); anonymous = cst.getString(5);   BigDecimal attempts = cst.getBigDecimal(6); System.out.println("userCode = " + userCode);    System.out.println("Return Code = " + value);  cst.close();   conn.close();

         if (value == null || value.equalsIgnoreCase("N")) {   String from = GlobalCC.emailFrom; String to = GlobalCC.emailTo;

            String subject = "SYSTEM SECURITY MESSAGE";  String messageText =  "Failed user " + userNameVal + " login operation ";

            String messageType = "FAILED-LOGIN";   BigDecimal userCodeVal =
```

```
(BigDecimal)session.getAttribute("userCode");   if (attempts.compareTo(new BigDecimal(3)) == 1 ||

attempts.compareTo(new BigDecimal(3)) == 0) { GlobalCC.RaiseErrorMessage("SECURITY VIOLATON...USER ACCOUNT DEACTIVATED..."); logAndSendViolationMessage(from, to, subject, messageText, messageType, userCodeVal);

} else { GlobalCC.RaiseErrorMessage("SECURITY VIOLATION...."); }  if (anonymous != null && anonymous.equalsIgnoreCase("Y")) { messageType = "ANONYMOUS-LOGIN"; messageText =

"Failed anonymous user " + userNameVal + " login operation ";  logAndSendViolationMessage(from, to, subject, messageText, messageType, userCodeVal);  }  return null;

} else {  Date today = new Date(); session.setAttribute("userName", userNameVal);  session.setAttribute("userCode", userCode);

session.setAttribute("lastLogin", today);  GlobalCC.redirect("home.jspx");  System.out.println("userCode = " + userCode);  }  } catch (Exception e) {  e.printStackTrace();  GlobalCC.RAISEEXCEPTION(conn, e);

}  return null;  }  public static String logAndSendViolationMessage(String from, String to,

String subject,  String messageText, String messageType, BigDecimal userCode) {

JavaMailer mailer = new JavaMailer(); String sentFlag =  mailer.sendSimpleMail(from, to, subject, messageText);

String messageDesc = messageText; String messageSender = "SYSTEM"; String messageReceiver = GlobalCC.emailTo; String messageStatus = "SENT";  BigDecimal messageUser = userCode; MessagesBean.updateMessages(messageType, messageDesc, messageSender, messageReceiver, messageStatus, messageUser);  return null;  }  public String loadUserPermissions() { return null;  }

public String resetPassword() { //To be called if the password expiry date is reached or if is a new user.

return null;  }  public static String userAuthenticate(String userNameVal, String passwordVal) {  DBConnector datahandler = null; datahandler = new DBConnector(); Connection conn;  conn = datahandler.getDBConnection();  String value = null; CallableStatement cst = null;  String query = "{ CALL userAuthenticate(?,?,?) }";

try { cst = conn.prepareCall(query); cst.setString(1, userNameVal); cst.setString(2, passwordVal);

cst.registerOutParameter(3, Types.VARCHAR);  cst.execute();  value = cst.getString(3);  cst.close();

conn.close();  } catch (Exception e) {  e.printStackTrace(); GlobalCC.RAISEEXCEPTION(conn, e);  }

return value;  }  public String logout() {  SessionBean sb = new SessionBean();

sb.invalidateVariables(); session.removeAttribute("userName");  session.removeAttribute("userCode");

session.removeAttribute("lastLogin");  GlobalCC.redirect("index.jspx");  return null;

}  public void setLoginPassword(RichInputText loginPassword) {  this.loginPassword = loginPassword;

}  public RichInputText getLoginPassword() {  return loginPassword;

}  public void setLoginUsername(RichInputText loginUsername) {  this.loginUsername = loginUsername;

}  public RichInputText getLoginUsername() { return loginUsername;  }

public void setLoggedUser(String loggedUser) {  this.loggedUser = (String)session.getAttribute("userName");

}  public String getLoggedUser() {  return (String)session.getAttribute("userName");

}  public void setLoginDate(Date loginDate) {  this.loginDate = (Date)session.getAttribute("lastLogin");

}  public Date getLoginDate() {  return (Date)session.getAttribute("lastLogin");  }}
```