Int. J. Communications, Network and System Sciences, 2011, 4, 152-163
doi:10.4236/ijcns.2011.43019 Published Online March 2011 (http://www.SciRP.org/journal/ijcns)

A User Identity Management Protocol for Cloud Computing Paradigm

Safiriyu Eludiora[1], Olatunde Abiona[2], Ayodeji Oluwatope[1], Adeniran Oluwaranti[1], Clement Onime[3], Lawrence Kehinde[4]

[1]*Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria*
[2]*Department of Computer Information Systems, Indiana University Northwest, Garry, USA*
[3]*Information and Communication Technology Section, Abdus Salam International Centre for Theoretical Physics, Trieste, Italy*
[4]*Department of Engineering Technologies, Texas Southern University, Houston, USA*
E-mail: {*sieludiora, aoluwato, aranti*}*@oauife.edu.ng, oabiona@iun.edu, onime@ictp.it, kehindelo@tsu.edu*
Received January 3, 2011; *revised February* 9, 2011; *accepted February* 11, 2011

Abstract

Cloud computing paradigm is a service oriented system that delivers services to the customer at low cost. Cloud computing needs to address three main security issues: confidentiality, integrity and availability. In this paper, we propose user identity management protocol for cloud computing customers and cloud service providers. This protocol will authenticate and authorize customers/providers in other to achieve global security networks. The protocol will be developed to achieve the set global security objectives in cloud computing environments. Confidentiality, integrity and availability are the key challenges of web services' or utility providers. A layered protocol design is proposed for cloud computing systems, the physical, networks and application layer. However, each layer will integrate existing security features such as firewalls, NIDS, NIPS, Anti-DDOS and others to prevent security threats and attacks. System vulnerability is critical to the cloud computing facilities; the proposed protocol will address this as part of measures to secure data at all levels. The protocol will protect customers/cloud service providers' infrastructure by preventing unauthorized users to gain access to the service/facility.

Keywords: Cloud Computing, Confidentiality, Integrity, Availability, Identity Management, Authentication

1. Introduction

In cloud computing, resources are provided as a service over the Internet to customers who use them as when needed basis. Computing services are available through data centers and accessible anywhere, so that the cloud is a single point of access for tools that address the entire customer's computing needs.

The cloud—characterized by large scale complexes for data storage and processing, delivery of software as an online service and leveraged connection of wireless devices to services and applications offered online—promises systemic and economic changes for business. As customers generally do not own the computing infrastructure but access or rent cloud computing services, cloud computing minimizes capital expenditure and lowers barriers to entry. By uncoupling computing tools from physical location, cloud computing enables users to access data and systems regardless of geography or available media [1].

Cloud management—To conduct business ***within*** a cloud (recognizing what is available today), it is important for cloud consumers and providers to align on graduated SLAs and corresponding pricing models.

Maturing cloud capabilities into more advanced offerings, such as virtual supply chains, requires support for fully abstracted, policy-driven interactions ***across*** clouds. It will become a major challenge for the cloud providers to adequately model, expose and extend policies in order to provide integrated services across distributed and heterogeneous business processes and infrastructure. The data associated with these business processes and infrastructure will need to be managed appropriately to address and mitigate various risks from a security, privacy, and regulatory compliance perspective. This is particularly important as intellectual property, customer, em-

ployee, and business partner data flows across clouds and along virtual supply chains [2].

"Cloud computing is the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. Sometimes known as utility computing, clouds provide a set of typically virtualized computers which can provide users with the ability to start and stop servers or use compute cycles only when needed, often paying only upon usage" [3]. **Figure 1** shows a typical used case scenarios architecture. There are service provider, service consumer, and service developer. Within the service provider there is security and management. Our focus is security with emphasis on identity management. In this paper, a scenario of an organization is considered. The identity provided for that employee must be used for every purpose that warrants the use of ID. Therefore, most of the existing IDM cannot be used for all situations. The federated IDM sounds appropriate. The federated IDM need to be enhanced high level of security.

1.1. Benefits of Cloud Computing

To deliver a future state architecture that captures the promise of Cloud Computing, architects need to understand the primary benefits of Cloud computing:

• Decoupling and separation of the business service from the infrastructure needed to run it (virtualization).

• Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts.

• Elastic nature of the infrastructure to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.

• Cost allocation flexibility for customers wanting to move Capital exchange into Operational exchange.

• Reduced costs due to operational efficiencies, and more rapid deployment of new business services [4].

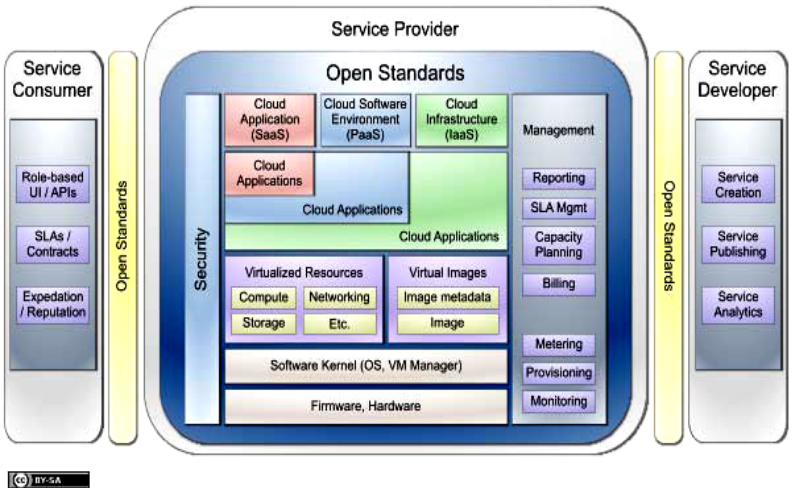
Cloud computing infrastructures can allow enterprises to achieve more efficient use of their IT hardware and software investments. They do this by breaking down the physical barriers inherent in isolated systems, and automating the management of the group of systems as a single entity.

Cloud computing is an example of an ultimately virtualized system, and a natural evolution for data centers that employ automated systems management, workload balancing, and virtualization technologies.

A cloud infrastructure can be a cost efficient model for delivering information services, reducing IT management complexity, promoting innovation, and increasing responsiveness through real-time workload balancing.

The Cloud makes it possible to launch Web 2.0 applications quickly and to scale up applications as much as when needed. The platform supports traditional Java™ and Linux, Apache, MySQL, PHP (LAMP) stack-based applications as well as new architectures such as Map-Reduce and the Google File System, which provide a means to scale applications across thousands of servers instantly.

Large amounts of computer resource, in the form of Xen virtual machines, can be provisioned and made available for new applications within minutes instead of days or weeks. Developers can gain access to these resources through a portal and put them to use immediately. Several products are available that provide virtual machine capabilities, including proprietary ones such as VMware, and open source alternatives, such as XEN [5].



Source: Cloud Computing Use Case Discussion Group

Figure 1. Cloud computing architecture.

1.2. Delivery Models and Security Issues of Cloud Computing

The NIST [6] definition of cloud computing defines three delivery models:

1.2.1. Software as a Service (SaaS)

The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running.

The SaaS model dictates that the provider manages the entire suite of applications delivered to end-users. Therefore SaaS providers are mainly responsible for securing these applications. Customers are normally responsible for operational security processes (user and access management). However the following questions, along with other sections within this document, should assist in assessing their offerings:

• What administration controls are provided and can these be used to assign read and write privileges to other users?

• Is the SaaS access control fine grained and can it be customized to ones organizations policy?

1.2.2. Platform as a Service (PaaS)

The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework. Generally speaking, PaaS service providers are responsible for the security of the platform software stack, and the recommendations throughout this document are a good foundation for ensuring a PaaS provider has considered security principles when designing and managing their PaaS platform. It is often difficult to obtain detailed information from PaaS providers on exactly how they secure their platforms – however the following questions, along with other sections within this document, should be of assistance in assessing their offerings.

• Request information on how multi-tenanted applications are isolated from each other—a high level description of containment and isolation measures is required.

• What assurance can the PaaS provider give that access to your data is restricted to your enterprise users and to the applications you own?

• The platform architecture should be classic "sandbox"—does the provider ensure that the PaaS platform sandbox is monitored for new bugs and vulnerabilities?

• PaaS providers should be able to offer a set of security features (re-useable amongst their clients) – do these include user authentication, single sign on, authorisation (privilege management), and SSL/TLS (made available via an API)?

1.2.3. Infrastructure as a Service (IaaS)

The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them. As with personnel security, many of the potential issues arise because the IT infrastructure is under the control of a third party – like traditional outsourcing, the effect of a physical security breach can have an impact on multiple customers (organizations).

• What assurance can you provide to the customer regarding the physical security of the location? Please provide examples, and any standards that are adhered to, eg,. Section 9 of ISO 27001/2.

• Who, other than authorized IT personnel, has unescorted (physical) access to IT infrastructure?

For example, cleaners, managers, "physical security" staff, contractors, consultants, vendors, etc.

• How often are access rights reviewed?

• How quickly can access rights be revoked?

• Do one assess security risks and evaluate perimeters on a regular basis?

• How frequently?

▪ Do you carry out regular risk assessments which include things such as neighboring buildings?

▪ Do you control or monitor personnel (including third parties) who access secure areas?

▪ What policies or procedures do you have for loading, unloading and installing equipment?

▪ Are deliveries inspected for risks before installation?

▪ Is there an up-to-date physical inventory of items in the data centre?

▪ Do network cables run through public access areas?

• Do you use armored cabling or conduits?

▪ Do you regularly survey premises to look for unauthorized equipment?

▪ Is there any off-site equipment?

• How is this protected?

▪ Do your personnel use portable equipment (eg,. laptops, smart phones) which can give access to the data centre?

• How are these protected?

▪ What measures are in place to control access cards?

▪ What processes or procedures are in place to destroy old media or systems when required to do so?

• Data overwritten?

• Physical destruction?

▪ What authorization processes are in place for the

movement of equipment from one site to another?

• How do you identify staff (or contractors) who are authorized to do this?

▪ How often are equipment audits carried out to monitor for unauthorized equipment removal?

▪ How often are checks made to ensure that the environment complies with the appropriate legal and regulatory requirements [7,8]. In the next subsection we discuss different deployment models.

1.3. Deployment Models of Cloud Computing

The NIST definition defines four deployment models:

1.3.1. Public Cloud

In simple terms, public cloud services are characterized as being available to clients from a third party service provider via the Internet. The term "public" does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user's data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.

1.3.2. Private Cloud

A private cloud offers many of the benefits of a public cloud computing environment, such as being elastic and service based.

The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

1.3.3. Community Cloud

A community cloud is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

1.3.4. Hybrid Cloud

A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource non-business-critical information and processing to the public cloud, while keeping business-critical services and data in their control. [7]

1.4. Essential Characteristics of Cloud Computing

The NIST definition describes five essential characteristics of cloud computing.

1.4.1. Rapid Elasticity

Elasticity is defined as the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing power as they need. This is one of the essential characteristics of cloud computing in the NIST definition.

1.4.2. Measured Service

It is a measured service, aspects of the cloud service are controlled and monitored by the cloud provider. This is crucial for billing, access control, resource optimization, capacity planning and other tasks.

1.4.3. On-Demand Self-Service

The on-demand and self-service aspects of cloud computing mean that a consumer can use cloud services as needed without any human interaction with the cloud provider.

1.4.4. Ubiquitous Network Access

Ubiquitous network access means that the cloud provider's capabilities are available over the network and can be accessed through standard mechanisms by both thick and thin clients.

1.4.5. Resource Pooling

Resource pooling allows a cloud provider to serve its consumers via a multi-tenant model. Physical and virtual resources are assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter) [7]. In essence security is the key challenge in exploring the benefits of cloud computing.

In this paper, we proposed user-IDM protocol (U-IDM). This work review available literature and general issues on cloud computing environments. In Section 1 we discuss a general introduction; the section introduces the key areas of cloud computing, and deployment models. In Section 2 we discuss scientific overview of security and cloud computing Identity management. Section 3 describes the theoretical frame work and our research philosophy. Section 4 discusses the proposed algorithms, in Section 5 we describe the simulations. Section 6 outlined the results and the paper was concluded in Section 7.

2. Overview

In this section, we discussed security and IDM issues in cloud computing environment and steps to be taken by cloud services' providers and customers alike.

2.1. Security

Security is the most important part of the total solution and requires end-to-end security practices. From an identity and access perspective, the enterprise can provide an identity authentication service for its employees regardless of where the service resides, either internally or in the cloud computing environment. The company owns and manages the employee's identity repository and does not share identities with any other entity. The company provides a central point in managing an employee's identity, including password preset/reset/changes.

The company enhances identity and security protection by protecting an employee's confidential and credential information, because the identity federation approach allows the enterprise to manage its employee's access control policy—determining where single sign on (SSO) occurs, asserting trust appropriately, and sharing acceptable attributes between the identity provider and the service provider.

From an end user's perspective, remote access can reinforce security by using advanced authentication mechanisms (such as strong authentication or multifactor authentication) to prevent identity theft over the Internet, or to leverage the Host Checker to verify allowed hardware, thereby ensuring a safe environment [9]. This may be referred to as information security.

2.2. Information Security

Security is a property of a well-designed system according FISMA [10]. The term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [11] to provide confidence, integrity and availability for the users.

Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.

Availability: Ensuring timely and reliable access to and use of information to the users.

Security is not a feature; it is a property of a system. It results from thorough analysis of security requirements, sound architecture and design, and secure coding practices [12]. Personnel security also enhance these features, organizations need to comply with rules and regulations laid down by the cloud service providers for the cloud customers.

2.3. Personnel Security

The majority of questions relating to personnel will be similar to those one would have asked his own IT personnel or other personnel who are dealing with IT. As with most assessments, there is a balance between the risks and the cost.

- What policies and procedures do you have in place when hiring your IT administrators or others with system access? These should include:
  - pre-employment checks (identity, nationality or status, employment history and references, criminal convictions, and vetting (for senior personnel in high privilege roles)).
- Are there different policies depending on where the data is stored or applications are run? For example, hiring policies in one region may be different from those in another.
  - Practices need to be consistent across regions.
  - It may be that sensitive data is stored in one particular region with appropriate personnel.
- What security education program do you run for all staff?
- Is there a process of continuous evaluation?
  - How often does this occur?
  - Further interviews
  - Security access and privilege reviews
  - Policy and procedure reviews.

2.4. Security Issues of Cloud Computing

Despite the beauty of Cloud computing application service, as mentioned earlier, Cloud service subscribers, particularly for larger enterprises with corporate information security policies need to be enforced from time to time, they may want to consider getting a security assessment from a neutral third party before committing to a Cloud vendor.

Gartner [13] noted that Cloud computing is fraught with security risks and seven specific security issues are brought to the attention of potential Cloud service subscribers that they should raise them with their providers before actually selecting them:

Privileged user access—ask the providers to supply specific information on the hiring and oversight of privileged administrators, and the control over their access, because outsourced services usually bypass the "physical, logical and personnel security controls" which exert over in-house programs.

Regulatory compliance—the providers who refuse to undergo this scrutiny are "signaling that subscribers can

only use them for the most trivial functions", as subscribers are ultimately responsible for the security and integrity of their own data even when it is held by a service provider.

Data location—ask the providers if they will "commit to storing and processing data in specific jurisdictions and whether they will make a contractual commitment to obey local privacy requirements on behalf of the subscribers".

Data segregation—subscribers' data should be segregated with data from other customers as the Cloud is typically a shared environment. The service providers should provide data encryption as options and evidence on the corresponding encryption schemes were designed and properly tested by experienced specialists, as "encryption accidents can make data totally unusable".

Recovery—ask the providers if they have implemented and tested any disaster recovery procedures (DRP) which provides them with "the ability to do a complete restoration" and most importantly, "how long it will take" to execute the DRP [14]. Security attributes of cloud computing are discussed, so that the entire system is reliable and accessible to the users.

2.5. Network Security Attributes of Cloud Computing

These basic security issues are: authentication, authorization, auditing, confidentiality, integrity, availability and non-repudiation.

Authentication: is a process by which one entity verifies the identity of another entity. This can be a person or program. The authentication process can be done in three ways; something that user knows such as password or login name, something user has such as personal identification number (PIN) and something user is such as finger print. There is could be a message authentication system that determines the source of message. Another authentication process can be machine-to-machine, which can be client, server and/or mutual authentications. Client authentication involves the server verifying the client's identity, server authentication involves the client verifying the server's identity and mutual authentication involves the client and server verifying each other's identity. In the context of UCS, a web server can be authenticated, so that user can deal with a real website, and not an imitating (disguising) web server. Transport layer socket (TLS) can be used for this process.

Authorization: is the process that ensures that a person has the right to access certain resources. Users can not be allowed to access any resources without knowing the attributes of such users. Users can have access rights to resources; but the authority to do something is not within their reach. For example, a user can use ATM card to withdraw money from the ATM machine. Having been authenticated, he cannot withdraw beyond a recommended maximum irrespective of any amount he has in his bank account. Cloud computing uses these access control and authorization to regulate resources usage and minimize fraudulent practices [15].

Auditing: is a process of collecting information about user attempting access to a particular resource, or performs actions. The log in system must be able to record all actions performed on that resource. In case there is any problem, the log file can be checked to trace such a user out.

Confidentiality (*privacy*): is an act that keeps private or sensitive information from being disclosed to unauthorized individuals, entities or processes. In cloud computing environment, it is important to maintain transactions' secrecy, because e-payment instruments like visa are involved.

Integrity: is the ability to protect data from being altered or destroyed by unauthorized persons or processes during the course of transmission. This is important in cloud computing environment, because the mobile devices use air medium and for this reason, data must be well protected.

Availability: is the unhindered accessibility of a service. An online service is available if a user or program can gain access to the pages, data, or services provided by the site when they are needed. This is critical to UCS. Unavailability of a web site may hinder the on-going transactions and it may lead to loss of money and customers. Technologies such as load balancing hardware and software are aimed at ensuring availability [16].

Non-repudiation: is the ability to limit parties from refuting that a legitimate transaction took place. Since cloud computing transactions involve money, it is important that the customer commits himself by endorsing his/her signature [16,17]. It is obvious that these attributes may be difficult to achieve, we therefore proposed a "User Identity Management Protocol (U-IDMP). In this case the emphasis is on user attributes provided by the enterprises for cloud service providers to verify such a user.

2.6. User Identity Management

Whether an application runs on-premises or in the cloud, it typically needs to know something about its users. Toward this end, the application commonly demands that each user provides a digital identity, a set of bytes that describes that user. Based on what these bytes contain and how they're verified, the application can determine things such as who this user is and what they're allowed to do.

Many on-premises applications today rely on an on-premises infrastructure service, such as Active Directory, to provide this identity information. When a user accesses a cloud application, however, or an on-premises application accesses a cloud service, an on-premises identity usually won't work. And what about an application built on a cloud foundation? Where does it get its identity information?

An identity service in the cloud can address these issues. Because it provides a digital identity that can be used by people, by on-premises applications, and by cloud applications, a cloud identity service can be applied in many different scenarios. In fact, one indication of the importance of this kind of identity service is the number of cloud identity services available today. Accessing Amazon cloud services such as EC2 or S3 requires presenting an Amazon-defined identity, for instance, while using Google AppEngine requires a Google account. Microsoft provides Windows Live ID, which can be used for Microsoft applications and others, while BizTalk Services also offers its own identity service, which can be federated with others. Developers don't have complete freedom—cloud platforms are frequently tied to a particular identity provider—but the need for identity as a cloud service is clears [1].

2.7. Identity and Access Management

The following controls apply to the cloud provider's identity and access management systems (those under their control).

2.7.1. Authorization

• Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations (read/write/delete)?

• How are the accounts with the highest level of privilege authenticated and managed?

• How are the most critical decisions (e.g., simultaneous de-provisioning of large resource blocks) authorized (single or dual, and by which roles within the organization)?

• Are any high-privilege roles allocated to the same person? Does this allocation break the segregation of duties or least privilege rules?

• Do you use role-based access control (RBAC)? Is the principle of least privilege followed?

• What changes, if any, are made to administrator privileges and roles to allow for extraordinary access in the event of an emergency?

• Is there an "administrator" role for the customer? For example, does the customer administrator have a role in adding new users (but without allowing him to change the underlying storage!)?

2.7.2. Identity Provisioning

• What checks are made on the identity of user accounts at registration? Are any standards followed? For example, the e-Government Interoperability Framework?

• Are there different levels of identity checks based on the resources required?

• What processes are in place for de-provisioning credentials?

• Are credentials provisioned and de-provisioned simultaneously throughout the cloud system, or are there any risks in de-provisioning them across multiple geographically distributed locations?

2.7.3. Management Personal Data

• What data storage and protection controls apply to the user directory (e.g., AD, LDAP) and access to it?

• Is user directory data exportable in an interoperable format?

• Is need-to-know the basis for access to customer data within the cloud provider?

2.7.4. Key Management

• For keys under the control of the cloud provider:

• Are security controls in place for reading and writing those keys? For example, strong password policies, keys stored in a separate system, hardware security modules (HSM) for root certificate keys, smart card based authentication, direct shielded access to storage, short key lifetime, etc.

• Are security controls in place for using those keys to sign and encrypt data?

• Are procedures in place in the event of a key compromise? For example, key revocation lists.

• Is key revocation able to deal with simultaneity issues for multiple sites?

• Are customer system images protected or encrypted?

2.7.5. Encryption

• Encryption can be used in multiple places—where is it used?

- data in transit
- data at rest
- data in processor or memory?
- Usernames and passwords?

• Is there a well-defined policy for what should be encrypted and what should not be encrypted?

• Who holds the access keys?

• How are the keys protected?

2.7.6. Authentication

• What forms of authentication are used for operations requiring high assurance? This may include login to management interfaces, key creation, access to multi-

ple-user accounts, firewall configuration, remote access, etc.

• Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc?

2.7.7. Credential Compromise or Theft

• Do you provide anomaly detection (the ability to spot unusual and potentially malicious IP traffic and user or support team behavior)? For example, analysis of failed and successful logins, unusual time of day, and multiple logins, etc.

• What provisions exist in the event of the theft of a customer's credentials (detection, revocation, evidence for actions)?

2.8. Identity and Access Management Systems Offered to the Cloud Customer

The following questions apply to the identity and access management systems which are offered by the cloud provider for use and control by the cloud customer.

2.8.1. Identity Management Frameworks

• Does the system allow for a federated IDM infrastructure which is interoperable both for high assurance (OTP systems, where required) and low assurance (e.g. username and password)?

• Is the cloud provider interoperable with third party identity providers?

• Is there the ability to incorporate single sign-on?

2.8.2. Access Control

• Does the client credential system allow for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities)?

• How do you manage access to customer system images—and ensure that the authentication and cryptographic keys are not contained within in them?

2.8.3. Authentication

• How does the cloud provider identify itself to the customer (*i.e.*, is there mutual authentication)?

▪ when the customer sends API commands?

▪ when the customer logs into the management interface?

• Do you support a federated mechanism for authentication?

End Users need to access certain resources in the cloud and should be aware of access agreements such as acceptable use or conflict of interest. In this model, end user signatures may be used to confirm if someone is committed to such policies. The client organization should run mechanisms to detect vulnerable code or protocols at entry points such as firewalls, servers, or mobile devices and upload patches on the local systems as soon as they are found. Thus, this approach ensures security on the end users and on the cloud alike.

However, the cloud needs to be secure from any user with malicious intent that may attempt to gain access to information or shut down a service. For this reason, the cloud should include a denial of service (DOS) protection. One way of enforcing DOS protection is done by improving the infrastructure with more bandwidth and better computational power which the cloud has abundantly. In the more traditional sense, it involves filtering certain packets that have similar IP source addresses or server requests. The next issue concerning the cloud provider to end users is transmission integrity. One way of implementing integrity is by using secure socket layer (SSL) or transport layer security (TLS) to ensure that the sessions are not being altered by a man in the middle attack. At a lower level, the network can be made secure by the use of secure internet protocol (IPsec). Lastly, the final middle point between end users and the cloud is transmission confidentiality or the guarantee that no one is listening on the conversation between authenticated users and the cloud. The same mechanisms mentioned above can also guarantee confidentiality [18].

2.9. Related Works

Identity federation is evolving to meet business globalization strategies, enterprise and cloud service providers are looking for best practices related to the cloud computing environment. In their paper, the authors demonstrated how remote access, identity management, and security can work together to enable, secure, and integrate cloud computing services. Four patterns were proposed and implemented. With the use of integration patterns, the enterprise can effectively design identity federation solutions in a hybrid cloud environment for different use cases specific to the business. Our critical study on the proposed patterns enables us to draw our conclusion that this work will give room for credential compromise or theft [9].

Adoption of IDM in cloud computing environments imposes challenges. The complexities that may be experienced by the enterprise in the management of ID couple with the other factors have over head costs. According to [18] IDM IaaS is user centric identity management and is being considered as a complete all-round solution addressing all possible issues of cloud IDMs. The authors were of opinion that it should be outsource to other companies that can effective manage them. Our view on this work is that IDM IaaS may not be enough to

address this security challenges, because the paper did not consider the other models like PaaS and SaaS. These two models also require appropriate IDM. Since cloud computing environments require holistic security, privacy and trust approach to earnest the benefits derivable from cloud computing.

3. Theoretical Framework

The development of user identity management protocol intends to answer some questions being asked by stakeholders and developers. Some these questions are on authorization, authentication, encryption, key management identity provisioning etc. We attempt these questions in our architecture and the U-IDM protocol developed. Our approach in solving these challenges that raised some questions is to develop a "user identity management protocol that will involve stage by stage transactions' verification of the customers. We considered authentication, authorization and accounting (AAA) in developing this protocol. These 3A are crucial to the implementation of any protocol in cloud computing environments. **Figure 2** describes our U-IDM protocol. The stakeholders work together to achieve successive transactions by monitoring the security of their infrastructural networks. The stakeholders are cloud service providers, registry, metering, billing, and customers. Bank and ISPs and others are not left out.

3.1. Cloud Services' Providers

The cloud services' providers determine conditions to release/provide any service. The security and IDM of the services' providers must be provided at different levels. The organizations registering their companies with service providers must have good service level agreements (SLAs) to prevent intrusions. The employee of any organization representing such organizations must be provided with adequate identifiable attributes that can be used to trace in case of any security bridge. Hence, end to end security must be maintained. The services' providers relate well with the registry. The unit authorizes the release of any service(s).

3.2. Cloud Services' Registry

The cloud services' registry registers all available services in the cloud computing environments. The registries maintain all the services and make them available to the customers. The services' providers determine the services to release to the customers. The registry consults with the services' metering unit to determine the payment indices.

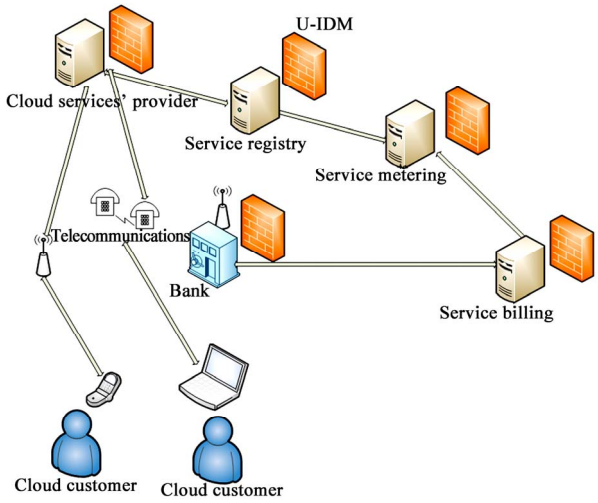


Figure 2. User identity management protocol architecture.

3.3. Cloud Services Metering

This unit provides all necessary parameters or formula to determine what a customer will pay on the service being requested for. The service type will be provided by registry unit. The services' details will be prepared and send to the billing unit.

3.4. Cloud Services Billing

This unit prepares the bill that the customer will pay. This information will be sent to the customer through service provider.

3.5. Cloud Services Customers

Customer get the bill make the payment through the bank and the bank sends the payment confirmations to the service provider.

3.6. Banks

Banks play significant in any transactions. Banks represent all of them in term fund raising and payment. Today, online banking make business easier through the Internet service providers or network operators.

3.7. NOs/ISPs

The Internet service providers or network operators are pivot that determine the direction of every transactions today. At every level, they should provide adequate security.

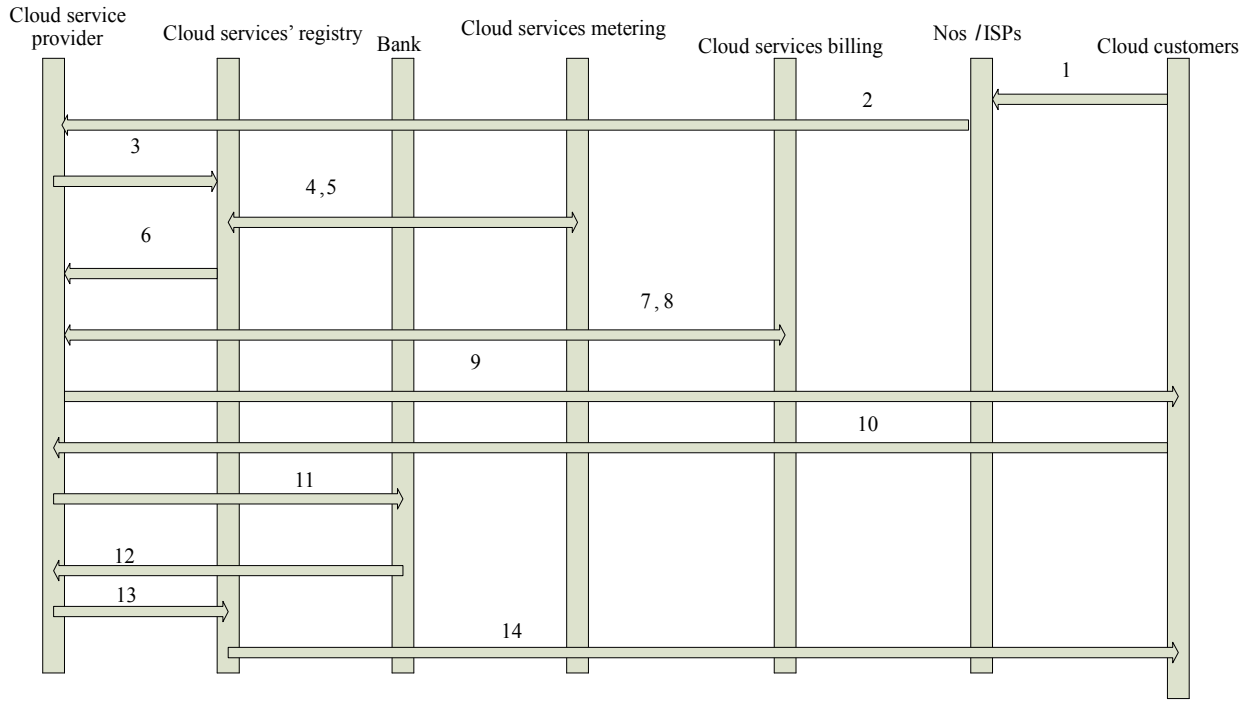
Having discussed the functions and relationships between stakeholders, **Figure 3** is the user identity man-

agement protocol. The protocol shows the relationship and transactions among the stakeholders. In addition, **Figure 4** explains the layers developed to support this protocol. The physically layer has provision for time sensitive/insensitive applications by providing TCP/UDP transmissions options. The network layer takes care of different network connections that may be used by the customers *i.e*. GSM operators and Internet service providers. At this layer, a common protocol is adopted thereby allow effective and good quality of services to the customers. The network operators provide appropriate security measures. This is to prevent system vulnerability, threats and attacks. Here verification take place, hardware and software are authenticated before it is being transmitted to the application layer. Also, integration of other security software is used at this layer. The use DIDS/NIPS, anti-virus and possibly Firewalls at this level is crucial to the successful of services' delivery and quality of service in the cloud computing environments.

4. Algorithm

(Pattern Matching) P and T are strings with lengths R and S, respectively and are stored as arrays with one character per element. This algorithm finds the INDEX of P in T.

1) [initialize]. Set K:= 1 and MAX := S – R + 1.
2) Repeat Steps 3 to 5 while K ≤ MAX:
3) Repeat for L = 1 to R: [Tests each character of P].
If P[L] ≠ T[K + L - 1], then Go to Step 5.
[End of inner loop].
4) [Success]. Set INDEX = K, and Exit.
5) Set K := K + 1.
[End of Step 2 outer loop].
6) [Failure]. Set INDEX = 0.
7) Exit.



Actions:
1: customer sends request to cloud service provider through ISPs
2: authenticate (verify) customer's device/attributes and forward the request to the provider
3: cloud service provider authenticates the customer and forwards the request to cloud services' registry for provisioning and service confirmation
4: cloud services' registry send the request to the cloud services' metering unit to determine the cost implications
5: the metering unit sends the cost implications back to services' registry
6: services' registry sends it to service provider
7: service provider forward the request to the billing section
8: billing section determines the amount to be paid and send it back
9: service provider forward the amount and other payment detail information to the customer
10: customer returns payment details to the service provider
11: service provider sends the payment details to the bank
12: the bank acknowledges the payment details and sends the confirmation to the service provider
13: service provider sends the payment confirmation to the services' registry
14: services' registry authorized the transaction and provides the service to the customer.

Figure 3. User identity protocol stakeholders' relationship.

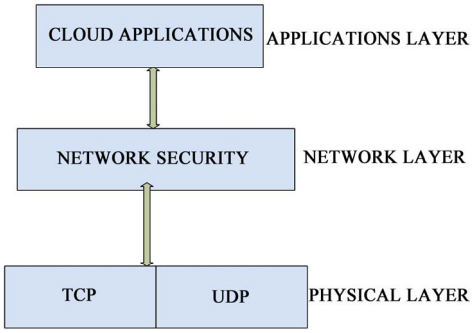


Figure 4. User identity management protocol layers.

5. Simulations

We simulate the algorithms using **Table 1** below. Different organizations employees' attributes were tested character by character to determine the successful match rate (SMR) failed match rate (FMR). This illustrates those services' providers that have weak, strong and very strong IDM in their end. This test is important for cloud customers to determine what levels of SLAs to agree upon.

6. Results and Discussion

The results show that when 100 tests were performed for the successful and failed attributes. The weak has higher percentage of failure and less percentage of success. The weak has about 4.5% fail and about 2.7%. Below 40 tests are not considered to be significant. They were used as control experiments. These are illustrated in **Figures 5** and **6**.

7. Conclusion and Future Work

We presented U-IDM protocol that will accommodate all the stakeholders. The algorithm used checks the customer attributes character by character. The simulations' results for weak, strong and very strong show that failed match rate and successful match rate have a wide margin.

Table 1. Customer attributes.

IdmEmployee
FirstName
Surname
DOB
EmployeeID
PositionTitle
CostCentre
Branch
Section
Department

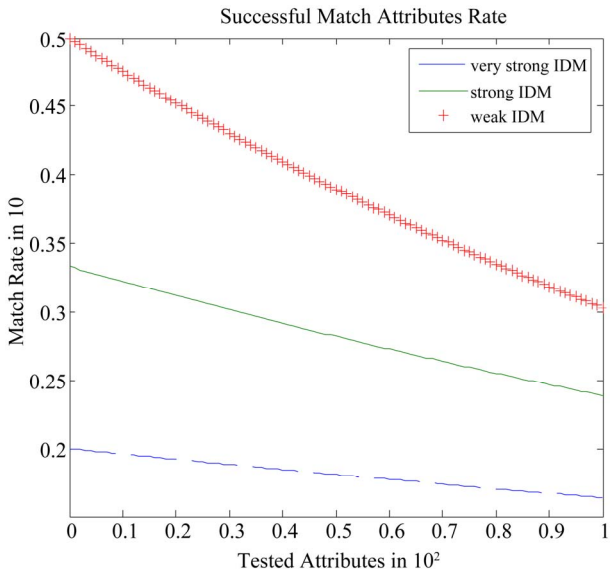


Figure 5. The successful attributes tests.

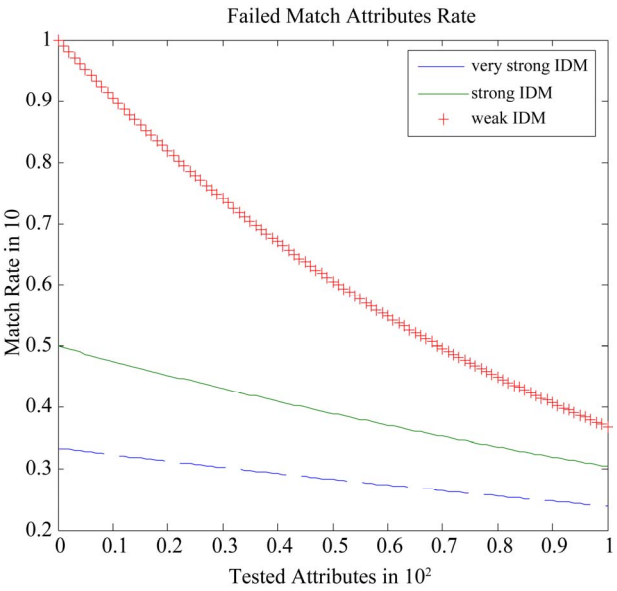


Figure 6. Failed attributes tests.

Considering when we test for 100 employees from different organizations, **Figure 5** has about 2.7% match rate for weak IDM and **Figure 6** has 4.5% match rate. We proposed that every participants of cloud computing must develop their own U-IDM. In future, we will work on the billing scheme for the cloud computing services.

8. References

[1] D. Chappell, "A Short Introduction to Cloud Platforms An Enterprise—Oriented View," Chappell and Associates, San Francisco, 2008, pp. 1-13.

[2] T. B. Winans and J. S. Brown, "Cloud Computing: A Collection of Working Papers," Deloitte Consulting LLP, New York, pp. 1-27.

[3] Stratus Technologies, "Server Virtualization and Cloud Computing: Four Hidden Impacts on Uptime and Availability," A White Paper by Stratus Technologies, June 2009.

[4] Oracle, "Architectural Strategies for Cloud Computing," An Oracle White Paper in Enterprise Architecture, August 2009.

[5] G. Boss, P. Malladi, D. Quan, L. Legregni and H. Hall, "Cloud Computing," IBM Corporation, New York, August 2007.

[6] NIST, January 2010. http://www.nist.gov/

[7] P. Mell and T. Grance, "Effectively and Securely: Using the Cloud Computing Paradigm," NIST, Information Technology Laboratory, Boulder, December 2009.

[8] The European Network and Information Security Agency (ENISA**)**, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," November 2009. http://www.enisa.europa.eu/

[9] Juniper Networks, "Implementation Identity Federation in a Hybrid Cloud Computing Environment Solution Guide," October 2009.

[10] FISMA, January 2010. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[11] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[12] P. Bryden, D. C. Kirkpatrick and F. Moghadami, "Security Authorization: An Approach for Community Cloud Computing Environments," White Paper, November 2009.

[13] Gartner, "Assessing the Security Risks of Cloud Computing," 2009. http://www.gartner.com/DisplayDocument?id=685308

[14] S. So, "Cloud Computing and Information Security," *Info-Security Project*, No. 3, May 2009.

[15] G. Treu, F. Fuchs and C. Dargatz, "Implicit Authorization for Social Location Disclosure," *Journal of Software*, Vol. 3, No. 1, 2008, pp. 18-26.

[16] M. E. Whiteman and H. J. Mattord, "Principles of Information Security," 2nd Edition, Thomson Course Technology, Massachusetts, 2005.

[17] P. Venkataram and B. S. Babu, "An Authentication Scheme for Ubiquitous Commerce: A Cognitive Agents Based Approach," *Proceedings of IEEE Workshops on Network Operations and Management Symposium Workshops*, Salvador da Bahia, 7-11 April 2008, pp. 248-256.

[18] A. Gopalakrishnan, "Cloud Computing Identity Management," *SETLabs Briefings*, Vol. 7, No. 7, 2009, pp. 45-54.

