

Identity Management Framework for Open Distributed Environment

إطار إدارة الهوية في بيئة موزعة مفتوحة

by

Kamal Ahmed Al Karaki

Supervisor

Dr. Akram Al- Mashaykhi

**This thesis Submitted in the partial Fulfillment of the Requirement
of Master's Degree in Computer Science**

Computer Sciences Department

College of Computer Sciences and Informatics

Amman Arab University

2015





جامعة عمان العربية
AMMAN ARAB UNIVERSITY

Form (9)

College of Scientific Research and Graduate Studies

Authorization

We, the undersigned, pledge to grant Amman Arab University for discretion in the publication of the academic content of the thesis, so that the intellectual property rights of a Master thesis be back to the university in accordance with the laws, regulations and instructions relating to intellectual property and patent.


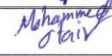

Advisor Name	Co-advisor Name	Student Name
Dr. Akram Al-Mashaykhi		Kamal Ahmed Al Karaki
Signature:  Date: 3/10/2015	Signature: Date:	Signature:  Date: 3/10/2015

شارع الأردن - موبص - عمان 11953 - ص.ب. 2234 عمان 11953 - الأردن
Jordan Street - Mubia - Telephone +962 7 8054 0040 - P.O.Box 2234 Amman 11953 - Jordan
Email: aaugs@aau.edu.jo / Web: www.aau.edu.jo

Committee Members' Decision

The thesis entitled: "IDENTITY MANAGEMENT FRAMEWORK FOR OPEN DISTRINUTED ENVIROMENT" was submitted by the student Kamal Al Karaki, was examined and approved on 22/9/2015

Committee Members

Name		Signature
Dr. Akram al Mashaykhi	Chair/Advisor	
Dr. Mohammad Otair	Member	
Prof. Asim Al Shaikh	External/ Member	

ACKNOWLEDGEMENT

The author would like to extend thanks to Doctor Akram Al-Mashaykhi, study supervisor for his patience, continuous advise provided and moral help, valuable comments, and academic guidance, without which, the completion of this work in time would have been difficult.

Sincere thanks are also due to the academic staff of the College of Computer Sciences and Informatics at the Amman Arab University.

Thanks are also due to colleagues and fellow post graduate students at the Computer Sciences Department.

Thanks are also due to my brother Dr. Mohamed Al Karaki for his assistant, continuous advise provided and moral help.

Last but not least the author is indebted to those who provided assistance at any stage of the postgraduate study.

DEDICATION

To the memory of my father.

To my mother for her love, encouragement and moral support.

To my wife Nagham for her love, help and moral support.

To my sons Ala', Laith, Ahmed and Qais.

LIST OF CONTENTS

AUTHORIZATION	II
RESOLUTION OF THE EXAMINING COMMITTEE	III
ACKNOWLEDGEMENT	III
DEDICATION	V
LIST OF CONTENTS.....	VI
LIST OF ABBREVIATIONS.....	VIII
LIST OF FIGURES.....	XI
LIST OF TABLES	XII
ABSTRACT	XIII
ABSTRACT IN ARABIC	XV
CHAPTER ONE	1
INTRODUCTION.....	1
1.1 PREFACE	1
1.2 SIGNIFICANCE OF THE STUDY	2
1.3 THE STATEMENT OF THE PROBLEM	3
1.4 METHODOLOGY AND APPROACH.....	4
1.5 THESIS OVERVIEW AND ORGANIZATION	6
CHAPTER TWO	7
LITERATURE STUDY	7
2.1 PREFACE	7
2.2 CLOUD COMPUTING	7
2.1.1 CLOUD COMPUTATION DEFINITION.....	7
2.2.2 CLOUD COMPUTATION CHARACTERISTICS,).....	9
2.3 IDENTITY MANAGEMENT	12
2.4 IDENTITY MANAGEMENT IN DISTRIBUTED ENVIRONMENT	15
2.5 LITERATURE REVIEW	18
MAIN FINDINGS OF THE LITERATURE REVIEW.....	38

CHAPTER 3.....	42
IDENTITY MANAGEMENT CHALLENGES, THREATS AND AVAILABLE SOLUTIONS.....	42
3.1 CLOUD COMPUTATION CHALLENGE AND THREATS:	42
3.2 IDENTITY MANAGEMENT CHALLENGES AND THREATS.....	45
3.2.1 INTERCLOUD RESOURCES IDENTIFICATION AND NAMING	46
3.2.2 IDENTITY INFORMATION INTEROPERABILITY IN THE INTERCLOUD	47
3.2.3 INTER-CLOUD'S LIFE CYCLE IDENTITY MANAGEMENT	49
3.2.4 INTERACTIONS OF SINGLE SIGN-ON IN THE INTERCLOUD	49
3.3 SOLUTIONS AVAILABLE TO MEET THE CHALLENGES AND THREATS IDM	60
3.4 STATE OF THE ART OF SOLUTIONS APPROACHES	64
3.4.1 FRAMEWORK DEFINITION	64
3.4.2 IDENTITY MANAGEMENT FRAMEWORKS	65
3.4.2.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML).....	65
3.4.2.2 LIBERTY ALLIANCE	68
3.4.2.3 WINDOWS CARDSPACE.....	71
3.4.2.4 PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE (PRIME)	74
3.4.2.5 OPENID	76
3.4.2.6 OAUTH	79
3.4.2.7 ONELOGIN	79
3.4.2.8 WINDOWS IDENTITY FOUNDATION (WIF).....	81
3.5 REVIEW OF IDENTITY MANAGEMENT FRAMEWORK IN CLOUD.....	82
CHAPTER FOUR.....	86
THE PROPOSED IDM FRAMEWORK.....	86
4.1 PREFACE	86
4.2 PRINCIPLES OF SELECTION IDM FRAMEWORK:	86
4.3 THE PROPOSED FRAMEWORK	90
4.3.1 THE FOUR BODIES INVOLVED IN FRAMEWORK	90
4.3.1 ORGANIZATIONAL CONTROL FRAMEWORK	92
4.3.3: ELEMENTS OF SECURE- CONTROL COMPONENTS	93
4.3.4 : PASSWORD SYNTAX RULES	95
4.3.4 SCENARIO OF WORKING FRAMEWORK	96
CHAPTER FIVE:	99
CONCLUSION AND RECOMMENDATIONS	99
5.1 CONCLUSION	99
5.1.1 GENERAL FINDINGS OF THE THESIS MAYBE SUMMARIZED AS FOLLOWS :.....	99
5.1.2 IDENTITY MANAGEMENT FINDINGS	100
5.2 RECOMMENDATIONS.....	101
REFERENCES.....	102

List of Abbreviations

Abbreviation	Meaning
ABE	Attribute Based Encryption
AFTCC	Architectural Framework for Trusted Cloud Computing
API	Applications Programming Interfaces
ASP	Active Server Pages
CEUA	CardSpace-enabled User agent (CEUA)
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DDoS attack	Distributed Denial-of-Service attack
DSML	Directory Services Markup Language
FIDIS	Future of Identity in the Information Society
FIM	Federated Identity Management
HTML	Hypertext Markup Language
IaaS	Infrastructure as a Service
ICT	Information Communication Technology
IdM	Identity Management
IdP	Identity Provider(IdP)
IP	Internet protocol
IT	Information Technology
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
NIST	U.S. National Institute of Standards and Technology

OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization
PaaS	Platform as a Service
PC	Personal Computer
PICOS	Privacy and Identity Management for Community Services
PII	Personally Identifiable Information
PRIME	Privacy and Identity Management for Europe
RBAC	Role Based Access Control
RFID	Radio-Frequency Identification
RP	Relying Party
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SEPs	Service endpoints
SICM	Simple Cloud Solution Management
SOAP	Simple Object Access Protocol
SP	Service Provider
SPML	Service Provisioning Markup Language
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSO	Single Sign- On
URL	Uniform Resource Locator
VO	Virtual Organizations

WIF	Windows Identity Foundation
WS	Web Services
XML	eXtensible Markup Language
XRDS	eXtensible Resource Descriptor Sequence
XRI	Extensible Resource Identifier

LIST OF FIGURES

Number	Content	Page
1	NIST Visual Model of Cloud Computing Definition	8
2	Identity Provider Initiated SAML Assertion Flowchart	68
3	Single-Sign-On	70
4	CardSpace Model of Identity Management	73
5	Execution of a transaction	75
6	OpenID Authentication protocol	78
7	Conceptual framework proposed by the study	90
8	Organizational Control Framework	92
9.a	Elements of Secure-Control component	93
9.b	Functions of Secure-Control component	94
10	Password Syntax Rules	94
11	Scenario of working framework	97

LIST OF TABLES

Number	Content	Page
1	Identity Management Challenge and threats	57
2	Available solutions for challenges and threats	63
3	Identity Management Frameworks & it's Attributes	82
4	Roles Matrix of bodies involved in IdM Framework	91

Identity Management Framework for Open Distributed Environment

Prepared by
Kamal Ahmed Al Karaki

Supervised by
Dr. Akram Al- Mashaykhi

ABSTRACT

Identity Management in Cloud computing is one of the most important security challenges for managing and assuring a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mechanisms, processes and policies.

Many researches on this subject were reviewed and found to be helpful in providing brief background on Identity Management in cloud computing and related issues. Some of these researches were theoretical (provided theory background basis about the subject). Others concentrated on the framework of research undertaken. But, the major pieces of work tackled methodology followed by previous researchers to introduce the main obstacles that hinder development of the sector and call for assistance.

This thesis describes the Identity Management challenges and threats and the available solutions, then propose an identity management framework which include Identity Management policy, bodies with multi

level of authority and roles, components each with cretin functionality and procedures and organizational control framework consist technical, legal and policy control that ensure the right information at a right time provided for the right parties and guarantee the security and privacy protection.

إطار إدارة الهوية في بيئة موزعة مفتوحة

إعداد

كمال احمد الكركي

اشراف

الدكتور اكرم المشايخي

الملخص

تعتبر إدارة الهوية في الحوسبة السحابية من أهم التحديات الأمنية لإدارة وضمان استخدام أمن للمصادر المتاحة من مزودي الخدمة في بيئة الأنظمة الموزعة المفتوحة والبنى التحتية المتخصصة للإتصالات وآليات الأمن والعمليات والسياسات المتعددة.

اجريت الكثير من الابحاث والدراسات حول هذا الموضوع، بعض هذه الأبحاث قدمت حلول نظرية لإدارة الهوية، بينما ركزت أبحاث أخرى على وضع اطر عمل للمساعدة في إيجاد الحلول المناسبة للعقبات الرئيسية التي تعيق تحقيق الأمن والخصوصية لإدارة الهوية عبر البيئة المفتوحة. كذلك تم وضع العديد من اطر العمل من خلال شركات متخصصة لإدارة الهوية في هذه البيئة ولكن جميع هذه الأطر والحلول كانت تعترضها بعض المحددات والمعيقات التي ظهرت من خلال التطبيق العملي لها.

ومن خلال هذه الأطروحة يتم استعراض أهم تحديات إدارة الهوية والتهديدات الأمنية والحلول المتاحة لها مع بيان المحددات والمعيقات لكل من هذه الحلول، ومن ثم اقتراح إطار عمل لإدارة الهوية في بيئة موزعة مفتوحة، يتضمن سياسة إدارة الهوية خلال أربع هيئات ذات مستويات متعددة من السلطة والأدوار، ومكونات كل هيئة ووظيفتها، كما يتضمن إجراءات وإطار الرقابة التنظيمية المكون من ضوابط تقنية وقانونية، بما يحقق الوصول للمعلومات الصحيحة في الوقت المناسب للجهة الطالبة مع ضمان اكبر قدر ممكن من الأمن والخصوصية .

CHAPTER ONE

INTRODUCTION

1.1 PREFACE

In both traditional and artifact systems, the question of identity play a very important factor and role in protecting and securing the people, operations, resources, systems and information. Introduction

With possibility of remote access to information systems and other ICT infrastructure this issue becomes more important, and as information and its operation become a strategic and competitive factor for any aspects of modern life, this issue becomes more crucial.

Identity Management with open system environment with multi users each with multi way of access to the system and application in term of access tools vary from work station to PCs, laptops, I pads and other smart devices, with IT as a service Model and Virtualization of infrastructure, platform and software service through Cloud computation service and deployment models such new environment bring a new threats and challenges to security management in general and to identity control and management in particular.

Several attempts to address this problem were conducted by both the scientific research institutes and by leading ICT companies, these attempts provide different approaches and different tools with different efficiency and

effectiveness measurements results and yet the subject open for farther effort for new and different and innovative methods, tools and product to cope with a very changing and demanding environment.

With the difficulties of controlling and managing the Identity based on the traditional and known methods and tools an increased demand for new different model to Identity management.

This work propose a model for Identity management stubble with specific set of requirements and constraints.

1.2 SIGNIFICANCE OF THE STUDY

One of the big concerns of ICT community all over the world is the identity management, and its related activities.

The importance of this study came out from the importance of the problem of defining a framework for IdM suitable for open environment, in order to protect and secure the information assets which became a vital factor of modern economy and national security and individual privacy, this work propose a solution framework model for the problem of identity management.

1.3 THE STATEMENT OF THE PROBLEM

Sustainable accessibility to systems, applications, and other information assets and resources due to increased numbers of persons with different organizational levels and authorities for several and different purposes and needs, all through increased type of smart devices from multipoint of access and yet the situation still evolving and diversified.

Such state of affair of multi people may access from multipoint, and multi location by using multi devices for multipurpose in different time the information systems complicate the scene and bring the threats sustainable too, and make the control and management of identity in order to protect the most valuable assets of any organization in the globe more and more difficult.

problem may be stated as follows: still there are some limitations and shortfalls in the all current solutions for identity management in open distributed environment. Thus a new insight or perspective and approach with help of new access control tools are become crucial in contemporary ICT environment and this is the problem to be embarking upon by this work by suggesting new framework and approach for new solutions, taking into account the findings of the related literature review that revealed a significant weakness and limitations accompanied with all current solutions, an issue that constitutes a major key of work of this study towards with constant solution to be suggested and practiced.

1.4 METHODOLOGY AND APPROACH

There are different kinds of identity management techniques that are used for preserving the privacy and discussing different Identity Management methods like PRIME (Privacy and identity management for Europe), Open ID, Microsoft Windows Card Space. Also there are limitations for them, such as a major limitation of the Window Cardspace is relying on single layer authentication and is relying on the third party, whereas, the main limitation of PRIME is that it requires user agents and service providers to implement the PRIME middleware, and OpenID is highly at risk of phishing attacks As in many IDMs, phishing in OpenID is of great concern. Even if passwords may be not transmitted with the security token, an attacker may trick the user into accessing the phisher's site and that site might accept any security token the user provided asking for information such as a credit card number. The phisher would not learn the user's password from the faked site, but he/she might learn other useful things.

This work applies the methodology stated hereunder:

1. Investigate the problem of IdM in general, and particular within the context of cloud computational model, in order to specify the scope, boundary, trends, challenges and possible solutions.

2. Determine the:
 - a. IdM landscape, standards, classification scheme , security measurement and entity authentication assurance.
 - b. Baseline capabilities and mechanisms of identity management for mobile applications and environment.
 - c. Open identity trust framework.
3. Define the Criteria for assessing the level of protection for personally identifiable information in identity management.
4. Examine available approaches, methods, tools and products of IdM.
5. Propose a Framework for open distributed environment, and give the requirement, justification, limitation, constraint related to the model.

1.5 THESIS OVERVIEW AND ORGANIZATION

This thesis consists of five chapters including the introductory chapter that contains of significance of study , statement of the problem, methodology and approach for this study.

Chapter two that contains: Concept and Background about cloud computation and Identity management in part one , and literature review and main findings in part two.

Chapter three includes cloud computation & identity management challenges and threats, available solutions for cloud computation & IdM challenges and threats, and state of art of solutions approaches (frameworks).

Chapter four present proposed framework .

And finally, chapter five covers the overview summary, conclusions and suggestions for further research.

CHAPTER TWO

LITERATURE STUDY

2.1 PREFACE

This chapter reviews cloud computing definition, characteristics, services and deployments; Identity Management and distributed environment identity management in part one. And illustrates literature review in part two, to benefit from their methodology and mean findings.

Part One: Concept and Background

2.2 CLOUD COMPUTING

Cloud computing phenomena and related conditions and environment have been under study by different scientists and researchers. Many pieces of research have been conducted to investigate such phenomena. A lot of papers were written on this subject. One of the main topics related to security of inter cloud is the identification of users and resources.

2.1.1 CLOUD COMPUTATION DEFINITION

U.S. National Institute of Standards and Technology (NIST) defines cloud computing as :

“Cloud computing as 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”. (The NIST Definition of Cloud Computing. (Peter & Timothy, 2011). Figure (1) shows NIST Visual Model of Cloud Computing Definition.

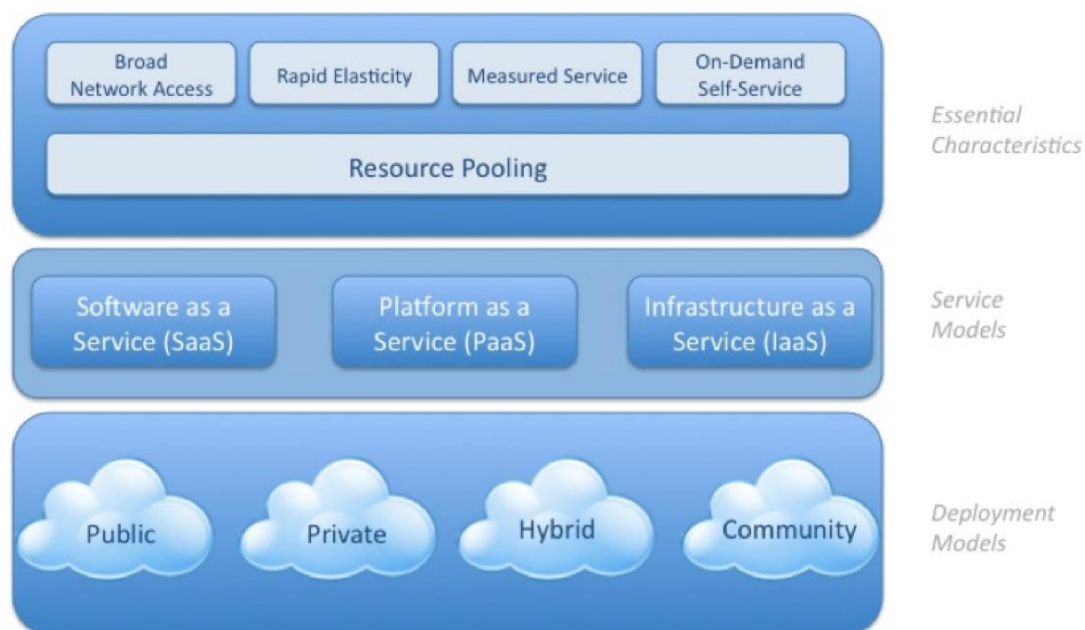


Figure (1): NIST Visual Model of Cloud Computing Definition

Cloud computation is based on Internet computation, where shared software, information and resources are offered to devices and computers on demand. It offers persons a way to share distributed services and resources that belong to various organizations. Since cloud computing is used the distribution of resources in an open environment, it is important to provide security and confidence for the exchange of data for development of cloud computing applications. This is an overview of cloud computing.

2.2.2 CLOUD COMPUTATION CHARACTERISTICS, SERVICE AND DEPLOYMENT MODELS. (PETER & TIMOTHY, 2011)

Cloud computation is to provide of computation services among the Internet. Services of Cloud allow persons and organizations to use hardware and software managed by third party in far-off locations. Services of cloud examples include social networking sites, online business applications, e-mails and online file storage. Model Cloud computing permit access to computer resources and information from anywhere a network connection is available when a network connection is available from anywhere. Cloud computation supports a common set of resources, containing data networking and computer processing power and storage space and applications and users specialized companies.

Model of cloud computation allows access to computer resources and information from any place a network connection was on hand. Cloud computation provide a shared common set of resources, like specialized corporate, computer processing power, storage space for data, user applications and networks.

NIST definition clarify five essential characteristics of cloud computation:

- 1) Pooling of Resources – means that customers draw from a pool of computation resources, Normally in far-off data centers.

- 2) Broad network access – allow it to provide services over the private networks or Internet , different kinds of capabilities were obtained over the networks and accessed by the standard mechanisms (for example laptops, mobile phones).
- 3) On demand self service - Organizations (customer) may be request, manage and used their own computation resources, like network storage and server time, automatically when needed without any human inter-action with each service provider.
- 4) Measured Service – Using of the services is measured, then customer can get the bill directly. Control of Cloud systems and optimize resources use automatically by supplying a metering capability. Resource usage may be reported, managed and controlled, providing transparency for the consumer and provider of the utilized services.
- 5) Fast flexibility - Services may be scaled smaller or larger, to the user. The capabilities available for supplying frequently seems to be unlimited and maybe bought every time in the quantity needed.

Cloud service models are:

- 1) Cloud Software as a Service (SaaS) - Applications together with any required network, operating system, software, hardware were hosted by service provider. This capability make it available to customers from various client devices through networks, as the Internet.

- 2) Cloud Platform as a Service (PaaS) – Hardware, network and operating system are offered, and customer develops or installs its own applications and software. This provides the ability to the client to deploy to cloud infrastructure by acquired applications that have been created using tools and programming languages offered by the providers.
- 3) Cloud Infrastructure as a Service (IaaS) - the customer develops or installs the software, operating system and applications for the hardware and network. This ability is provided to client to storage, provision processing, and other original computation resources, after which, the consumer can runs and deploys applications and operating systems.

The NIST definition defines four deployment models of cloud services:

- 1) Internal cloud (Private cloud) – The cloud resources is functioned for specific organization. It can be monitored and managed from a third party or the organization itself.
- 2) Community cloud – Infrastructure of the cloud is shared by many organizations and provides a community that sharing concerns. The infrastructure might be functioned and owned by a cloud service provider or the organizations itself.

- 3) Public cloud - cloud resources owned and operate by cloud provider like storage and applications. Then it will be available to public or a lot number of organizations. It is owned by an institute that sell cloud services
- 4) Hybrid cloud - which uses a mix of (community, private or public cloud) that remain unique entities, although bound collectively by a common technology that enables application and data.

2.3 IDENTITY MANAGEMENT

On the internet, each user has multiple profiles and have write access for many different applications, provided by different service providers. This make many challenges to the service providers and users, in forms of security, synchronization of shared identities, etc. However, a strong need for a trusted genuine identity system across the internet and unambiguously identifying users and within enterprises. Federation of identities maintained by the multiple service providers on the cloud is very essential to the application integration and cloud based service composition. In this respect, an expected issue is the naming heterogeneity. Different factors used by different service providers for authentication such as email ID, PayPal ID, account number, etc.

Previously, in classic environments the user identity mapping has been one-to-one, while it is one-to-many, many-to-one and pseudonyms in cloud environment. User uses a pseudonym when he does not want to his identity to be followed while he crusades various sites.

Another issue is setting of trust between the service providers in the federal world relationship. Currently, it is based on frame by the local authority policy files, depending on various factors like the domain trust information automatically fed in by the trust authorities. This model is inflexible, so it does not meet cloud computing demands. Scenarios of Cloud require dynamic authorization and dynamic trust propagation.

Identity Management is a job which is submitted to managerial of persons authentication in a system and right of entry resources authorization of the system reliant on the related restrictions and rights.

Because large number of customers and services exist, identity management is the essential activity in a cloud computing environment. Several persons are accessing to use cloud services. This requires managing and storing identities for security reasons and providing a trust based solution. So identity management task is to provide right of entry control to services based on attributes of resource and attributes of Users are essential for access control to services. Identity management systems are a great cloud computation environment federated concept of identity also involved a lot of

providers of cloud services to meet specific customer needs. To manage different identities for such a user in an environment is a challenge and difficult issue. Current system still have the concept of federation, which is not for cloud applications. in the Federal Cloud environments, must allow for setting the resources and users and also to interoperability support through multiple identity fields. In such a scenario, users should be able to access various services and resources provided by any providers of services, when they are authenticated in the Inter-Cloud interface (Christian et al., 2007). One obstacle associated with such situation is how to release users from the burden of authenticating with resources from multiple Cloud providers, that is, since each Cloud has a mechanism of authentication, a standard methods that provides Single Sign- On (SSO) authentication inside Inter-Cloud environments could be deployed. This must be applied both for provider-provider and customer-provider interactions. Achievement of SSO issue in federated environment occurs through the allocation of trust that allows a person to act on another person's behalf. This is very important. when services and resources of different service providers are involved in serving an Inter-cloud application, and it may be redundant, or very expensive to authenticate each and every time a user or application needs to access the resource. One method of delegating trust that is effectively used is to make use of proxy certificates.

Identity management object is very sensitive for cloud computation environment. The remote access and management of user credentials are creates privacy concerns and it causes many challenges and threats. (Naqvi et al., 2009) (David et al., 2011).

2.4 IDENTITY MANAGEMENT IN DISTRIBUTED ENVIRONMENT

Identity management in distributed environments, has been recognized challenge. An example of this issue is the emergence of cloud computing, and specifically federated inter-clouds, only on a much larger scale and requiring more general solutions. several projects and groups identify the motivations, motivations, challenges and issues surrounding Federated Identity Management (Massimiliano et al., 2012) (Bernstein & Vij, 2010).

In traditional IT environment, service provision of Identity management is able to perform either through what possessed by user, characteristics, attributes that make up the identity of the real world to the user, through something assigned to the user by a third party entity or by something the derives from a user's attainments and Passage. (Tewfiq & Jean, 2007) (Cao & Yang, 2010), this can be classified services required to facilitate identity management in these categories:

- a. Identity style service, where the user is identified using trust records, history access records, reputation, and honor .
- b. Identity service attribute, where the user is identified through specific attributes that are compatible with real-world entity
- c. Identity ID service, where the user is identified through the allocation of specific identifiers, like e-mail or identity card number.
- d. Identity accreditation service, where the user is identified through the adoption of a pre-set credentials like a digital certificates.

While we move on to grid computing and deployment of distributed systems, where it is the sharing of services and resource within Virtual Organizations (VO), identity management services have to support secure and seamless access to qualified users regardless the location the requested resource (PICOS, 2015) (FIDIS, 2015). on the basis of architecture, this identity management systems be able to classify as :

1. Centralize, wherever the central entity is in charge for the implementation of user defined, which is necessary for user identification and authentication. prior to accessing the requested service or resource, user must get authorization from this entity. This mandatory interaction brings up the disadvantages of this approach about privacy weaknesses and administration with the cross-domain access control and obstacle privilege delegation . The well-known

systems like this approach are PKI (Chang et al., 2001) and Kerberos (Kerberos, 2015).

2. Federate, That is based-on trust creation between the parties involved relationships. After all users mutually agree on standards, techniques and agreements, they form trust relationships and are then it is necessary to provide legitimate information for their users requested by other trust user. Each relying party be able to still select its favorite identification service. But, once the user is authenticated to the domain successfully, she/he has the ability to get personalized services through the federal domains, through the capability of her/his identity. Well-known systems depend on this approach involve Liberty Alliance Project (LAP, 2015), Shibboleth (Shibboleth, 2015) and Web Services Federation (WS-Federation, 2015).

Part two: Literature Review and Main Findings

2.5 LITERATURE REVIEW

Cloud computing phenomena and related conditions and environment have been under study by different scientists and researchers. Many pieces of research have been conducted to investigate such phenomena. A lot of papers were written on this subject. In the following paragraphs a summary briefing the literature review is provided.

Ajay & Prasun in 2013, realize that the feature of virtualization and large scale distribution has carried out the cloud computation idea. Regardless of its acceptance, most of the initiatives are still cautious regarding having clouds totally. This may be attributed partially to the features of identity. However, there are many who realize that it may be due to other factors such as access management, monitoring, auditing and reporting. The old-style access management will not serve in the cloud context indeed. Each initiative is in need for monitoring its staffs and related services, and this will help in the process of auditing. It is preferable to go for centralization in monitoring accompanied with a central access management at the enterprise level to assure coordination between contact management and observing as a service provided.

According to Yasir Saleem & et al in 2012, cloud computing is evolving technology with economic calculations with regard to associated infrastructure. It supplies the facilities based on of “as you pay as you go”. Confidentiality and safety are at the top level in the risk considerations in cloud data administration environment. Privacy of the data may be influenced when cloud users are not alert regarding the “location of the data kept on servers”, data isolation constitutes a major obstacle during the process of storing the data. Also, identity management may provoke a problem to be solved by the cloud users themselves, with all these issues in mind, their research proposed a model for improving the confidentiality in the cloud environment and security of the data. Single Sign on uses various identity management tools for improving the confidentiality and safety of the cloud operators including, OAuth, OpenId, and SAML etc. The paper pointed out the fact that safeguarding the identity management constitutes an important tool in the process of securing our permissions and entree management that provides security in the provision of the cloud data management situations.

Peering in mind the fact that : mitigation attack in cloud environment questions secure computation in cloud environment, Ushadevi & Rajamani in 2013, suggested a real time service and positioning tool with the purpose of accessing the cloud assets securely in the cloud environment. The identity

management, security situations, data management facilities are produced, collected and positioned at runtime. The active nature of the survive structure and organization provides safety for the service suppliers and cloud servers. The mentioned services collected are deployed in cloud servers in a selective way; the choice of server is done randomly. The cloud user may be achieved by the deployment of facilities in order to be able to make any required changes on their data that are out sourced them. However, it is worth mentioning that whatever the data, could be achieved only by the positioned facilities, there is no difference between the service suppliers or consumers. The paper concluded that the suggested technique may help reducing the internal attack and amount of guessing attack.

As mentioned earlier, cloud Computation is thriving daily and this booming is expected to continue in the future. Dealing with cloud computing raises some safety and circulation associated questions. Weight Harmonizing may answer such type of questions. RBAC work with these as well. Taking these ideas into accounts, Ruhi in 2014, suggested a tool that relates hybrid of FCFS with RBAC technique. RBAC may allocate parts to the consumers and consumers with a specific character may only have access to related specific document. The paper suggested that identity management and access management could be totally applied through this tool.

A research by Bing & Chengxiang in 2012, indicated that the moving developments of networks, particularly, Internet of Things, electronic identity management in cyberspace enjoys crucial role. Personal identity situations in cyberspace related to persons in real world has become substantial and crucial mission in the future growth of information creation in China. The paper proposes a RFID-based electronic identity security cloud podium in Internet to gadget a valuable security management of replicated individual identity, and plans and grasps a durable and persistent security cloud service platform, and argues key technology tools, including single-oriented spread, security cloud service, multi-level privacy protection instrument, great frequency RFID with electronic identity cards, security separation and security authentication methods for the electronic identity cards, and margin security entry protection, also it may be applies well to manage personal identity with the default roles of citizens in cyber-space like E-Business and E-Government, and the electronic identity security stand has been primary applied and achieved good possessions in submissions.

David & et al. in 2014 realized the fact that OpenStack is an open source cloud computation scheme with global acceptance. Where some cloud deployments may be detached, safe federated public clouds, (for example, inter-clouds), are required. So, there should be techniques for federated

identity management (FIM) to help in the authentication and authorization processes. This is to assure flexible enforce across federated environment, taking into account the presence of different FIM protocols today. The paper addresses the aim behind adding protocol sovereign united personality management to the OpenStack facilities. Characteristics of the cloud architectures delay usage of practices while achieving end-users' and companies' obedience needs taking into accounts infrastructural as well as commercial factors, such as sustainability in case of cloud-side interruptions, identity management and off-site corporate data handling policies. His article overviews recent attempts at formal definitions of cloud computing, summarizes and critically evaluates suggested definitions, and specifies obstacles related with its further explosion. Based on the conclusions achieved, future guidelines in the field of cloud computing are also briefly assumed to include deeper focus on community clouds and strengthening innovative cloud-enabled boards and procedures such as tablets, smart phones, as well as performing applications.

Prasanalakshmi & Kannammal in 2012, indicated that the difficulty of scheming, fitting, shaping, positioning, and supporting the system with resources may be abolished with this approach, supplying more benefits to agencies. But such models may raise some authentication difficulties for agencies that depend on outsourcing. The paper describes the application of

Security Assertion Markup Language (SAML) and its competences to supply Secure Single Sign-on (SSO) solutions for externally hosted applications, including security measures for federated identity management systems that use multifactor authentication, that also includes Biometric identification.

Ramkinker & et al. in 2013, highlighted the idea that cloud computation is spreading. Personal Health Record (PHR) is evolving in the surface. Due to sensitivity of the records kept, safety and efficient allocation practice are in need now. Patient information stored in a third party. Based on these facts, the writers suggested using Attribute Based Encryption (ABE) that can supply users with only required necessary information and disseminating the key of those characteristics". Taking into account the fact that Hacking of user profiles is a common scenario, they proposed introduction of a trust based dynamic reputation to further strengthen the security of PHR.

Elisa & et al. in 2013, highlighted the fact that digital identity management facilities are important in cloud computation infrastructures with the purpose of authenticating clients and provide supported supply access monitoring to facilities, based on previous interactions and users identity characteristics. This may help in the preservation of the users' confidentiality, while improve interoperability across fields and simplify

administration of identity certification. In their paper they suggested addressing such needs taking into accounts using zero-knowledge proof protocols, semantic matching techniques and high level identity verification policies given in the forms of identity attributes. Their paper also describes the major tools adopted and method of improvements.

Rizwana & Sasikumar in 2013, presented an analysis for different identity management systems and proposed a simple trust based program for cloud computation to be applied and put in service, the characteristics and techniques supplied by different suppliers made good market for the business, They concluded that different safety obstacles should be given more attention.

Libor in 2012, provided an overview on cloud computing, and indicated that cloud computing is a cost-effective option for acquiring and there is a rapid movement in the processing resources of corporations, scientific applications and individuals as well as different obstacles that should be fronted. While academia faces to obtain a brief description, businesses prefer to concentrate on competitive advantage it may obtain. Individuals see it as a way of raiding up data through times or a suitable backup solutions. Based on his conclusions achieved, future guidelines in the field of cloud computing are also briefly assumed to include deeper focus on community

clouds and strengthening innovative cloud-enabled boards and procedures such as smart phones, tablets, in addition to performing applications.

Pelin & et al. in 2010, realized that units (e.g., clients, facilities) should authenticate themselves to service suppliers to use their services as entities supply personally recognizable information as Personally identifiable information (PII) exclusively classifies it to an service suppliers. The researchers suggested an entity centric approach for Identity Management in the cloud based on unnamed identification (to mediate relations between cloud services and the entity using entity's confidentiality policies) and active bundles (each including privacy policies, a payload of Personally identifiable information , and a virtual machine that enforces the rules and uses a set of defense devices to guard themselves). The major features of this approach are: no third party required, give least amount information to the Service Provider and affords facility to use identity information on untrusted host.

Smita & Deep in 2014, discussed the confidentiality issue and various types of identity management tool used for conserving the privacy. Taking into consideration that cloud computation is supplying inexpensive on demand facilities to clients, pervasive network, large storage capacity due to these structures of cloud computing web applications are moving towards

the cloud, and because the web application migration, cloud computing platform raised a lot of matters as secrecy and safety. Thus, privacy matter is main concern for the cloud computation. Privacy is to maintain the perceptive information of the cloud consumers and the key issues of the privacy are the use of non-authorized secondary, absence of operator control, unclear responsibility. For dealing with these confidentiality issues Identity management method were used. The paper discusses the confidentiality issue and dissimilar kinds of identity management techniques used for maintaining the secrecy.

Andrew & Jeffrey in 2011, suggested that the applications in the markets are gradually wrapped as network facilities run in the cloud under a service providers control. Users of these services do not have sources in the determination if these services are reliable, beyond the assurances of the service provider. The paper showed how the user would be able to gain insight and trust into service application by leveraging trust in fair third party. A reliable cloud provider might be active as an origin of trust to show cloud hosted facilities to their customers reliable platform cloud. The researcher have prototyped this approach in a trusted platform as a service cloud provider supporting a Python/Django web framework .The cloud provider covers examples of service applications and shows their Python

source code to outside users. Once launched and attested, service instances run with an independent identity and are isolated from interfering by the cloud customer, except through well-defined operator borders that are part of the service categories and subject descriptors.

Mauro & Zair 2012, analyzed research works on access in a cloud computing environment. They indicated that authentication and access authorization should be prioritized in the area of computer security for protection of personal identifiable information contained in a cloud provider. Also, to protect users as well as providers of cloud services, security should be shared by reliable sources and also well-match with others in the federation. The researchers believe that this work explores the access control device in the cloud.

The paper by Sarah & et al. in 2013, performed a research aiming to evaluate cloud computing to lay the basics of an "Architectural Framework for Trusted Cloud Computing" (AFTCC) that will allow businesses to lower their expenses by outsourcing their processes on-demand by verifying the confidentiality and integrity of their data and computation.

Having focused on creating the Software Architecture for trustworthy Cloud Computation, the research shows the weaknesses and strengths defined in the previous works that performed until now in Architectural

Framework for Trusted Cloud Computing and its elements and the way they fit in, and defines the most recent systems and researches that follow it to some degree.

The paper prepared by Ardi in 2014, discusses identity management became a critical subject in the cloud computing environments, that usernames, passwords and other data that is used to distinguish, authorize, and authenticate users for a lot of different hosted applications needs to be controlled by cloud providers. The fact that all the breaches that existed on non-cloud solutions are existent in the cloud at the moment was pointed out by the article, and other problems and breaches have been introduced as individuals are able to manage identities of users when they send data to the cloud. The identity management of users when they receive information from the cloud would be second. And, Identity management when information is transferred from cloud to cloud would be third. The article examined some of the well-known identity management systems, together with a few well-known cloud providers and their hard works together with some known cloud providers and the efforts to regulate their exclusive identity solutions using some of the pertinent technologies as Simple Cloud Solution Management (SICM), Security Assertion Markup Language (SAML).

Janaki & Durga in 2013, in their paper, demonstrates a rising method, named user centric identity management, that concentrates on cost effectiveness and usability from the point of view of the user. A few of the identity models demonstrated before, particularly, the federated model, were due to the necessity of simplifying the user experience. The main notes from this paper are that, although there are many realistic issues related to dynamic security. The research concentrates on deriving a better method which targets these concepts, and gives a practical solution for the cloud computing security dangers. The purpose of this research is to enhance cloud security by utilizing identity based cryptography in user centric identity management. The paper indicated that an entirely new method is required for the improvement of users. It seems ordinary to put forward the automation of identity management at the user's side. However that users might manage an inevitably increasing amount of credentials and passwords by memory or other elementary ways is totally fictional.

Roshni & et al. 2013, studied cloud computation as a new trend of computation concept that presents a scalable resources on demand. It is being under attacks and have risk for data confidentiality. The researchers reviewed different identity management frames that proved to be helpful in making cloud environment more safe.

The main remarks of this study writers were:

- 1) Identity Management System provides the management with multiple digital identities. And decides how to reveal individually particular information (PII) of entities to obtain exact service.
- 2) IDM does the following tasks :
 - a) Set up identities: comparing individually particular information with a user.
 - b) Describe identities: delegate attribute identifying a user.
 - c) Record the uses of identity data: store the personality movement in a system.
 - d) Destroy an identity: after the completion of the work personally identifiable information of the user become unusable.
- 3) Identity Management use one of these categories of identifiers:
 - a. Identifiers that both a user and Service Provider know.
 - b. Identifiers known by Providers may verify via these providers.
 - c. Identifiers that an entity is unique markers(on example retina).

Adrian & et al. 2007, The contribution of this paper may be shown in the technology to be used to directly improve and support the process of federated identity assertion. The technologies used connect earlier work on policy enforcement and model based assurance, on the believe that such technologies address identity management in various methods apart from usual focus for Identity Management, which frequently address or improve. with no addressing the identity assurance matters. It is improbable that federated identity systems will be applied for lots of enterprise duties. The problems of federated identity assurance are not frequently discussed.

Based on the findings paper concluded that :

- 1) Federated identity management constitutes problematic area, taking into account technology, standardization and research.
- 2) Identity assurance puts important, different and often ignored viewpoint on the problem, indicating that frames for assurance become essential.
- 3) There is big scope for using technology for shaping and defining framework.
- 4) Particular. The assurance modelling toolset indicates how one be able to use technology to determine what information needs to be shared.

- 5) Finally, the significance of automation of controls in easing running costs (availability of enhanced audit information and modifying risk mitigation landscape) is highlighted.

Kari in 2009, pointed out the main problems facing cloud computation as follows :

- 1) Services as Facebook, MySpace and YouTube are more or less well-known to everybody, of course there is Google, which launches new services all the time. However, this vast amount of services create a problem, Internet users have to be active to remember the many pairs of user name/password of these different services.
- 2) As of security outlook, main problem in OpenID seems to be its weakness in the application.

The major results of the paper were as follows:

- 1) Majority of the applications need information concerning users than just an identifiers.
- 2) Such information may be generated either by users who input the values or from attributes received through authentication.
- 3) Storing these values locally creates duplication of the information and pushes users to maintain them manually.

- 4) OpenID has obtained amounts of popularity. With popular service suppliers starting supporting it, it became popular. However Its strength (being open) has become its limitation.
- 5) If service needs any additional information, it may generate that from user, confirm it, when it is necessary, and store it locally.
- 6) Protocol's weakness for phishing is also an issue to be studied and solved.

Audun & et al. in 2007, summarized the major problems facing cloud computing as follows:

- 1) The quick growth in the number of online facilities that leads to increasing numbers of various identities needed by every user to manage.
- 2) Lots of people feel overloaded with identities and badly affected from password exhaustion, a problem that makes people unable appropriately control and protect their digital identities against identities theft.
- 3) Lots of identity management systems are planned to be scalable and cost effective from the view of the service provider (indicated Service Provider in future), which sometime create poor usability and inconvenience from the users' perception.

4) Being Service Provider centric, traditional identity management systems have largely overlooked the fact that very frequently, equally important for users to be able to authenticate Service Providers, the same for Service Providers to authenticate users.

The paper proposed a general approach to make users better and be able to control and manage their identities, as well as in the creation of more secure identity management solutions. In particular, a user-centric approach based on hardware and software technology on the user-side, aims at helping users accessing online services.

A quantitative research by Simon & Stuart in 2014, aiming to determine the relationship between the organizations' security management framework and the virtualized environment's security conditions was used by Simon Tran, Stuart Gold who worked on the problems of Virtualization Security. Their study aimed to examine the relation without manipulating the examined situation, descriptive quantitative research becomes the best way to examine the situation. The approach tackled the problem statement of the research by requiring an explanation of the relationship among variables. The research's results showed the quality of information system leadership to the IT managers. IT managers have to enhance their skills consistently.

They must also look for ways that might work better in training and obtaining knowledge.

This research proposed that the virtualized environment was for server platforms. Virtualizing end users' workstations or servers in demilitarized zone will create a vague area. Should server IT managers have the environment from the support and security perspective? Alternatively, should that environment be shared, and how would it be shared? Such questions require much more research in the field.

Amir & Thomas in 2005, proposed a Framework for an Interoperable Electronic Identity Management System, considering that electronic identity (eID) tokens have been rolled out to the citizens of several member states in the European Union (EU). Giving a method of Identification, Authentication and electronic Signatures (IAS) to individuals for online transactions is the primary aim of these eID tokens. Member States made heavy investments to build the e-government and the infrastructure services to support eID tokens. Meanwhile, the electronic identity management systems of Member States lack the wanted interoperability aspect. After studying the current system, the researchers proposed a simple solution to solve some of the major interoperability problems.

The paper suggested a framework that provides an interoperable solution that could be accepted publicly if it met some simple conditions. The solution

must be able to grant advanced security but not compromise the privacy of citizens.

The paper considered eID tokens to be the upcoming linking tools between citizens and public sector and concluded by saying that they are being issued to citizens across Europe by Governments. The framework provided solid steps to secure citizen's privacy while granting better security.

Harshit & Sathish in 2015, suggested a Control Framework for Secure Cloud Computing, and indicated that the big uprising technology in the Information Technology (IT) industry is Computing, and that it will affect businesses of any size, but the security problems will still make a big threat on it. The privacy and security problems existing in cloud computing have been proven to prevent its widespread adoption. The paper viewed these problems from a business perspective and the way they damaged the names of large companies. From the available literature review on current problems in cloud computing and the way they are dealt with by the Cloud Service Providers (CSP), the studiers proposed a governing body framework designed to solve those problems by creating a relationship through the CSPs where the potential threats on data might be generated using past attacks on other CSPs. The proposed governing body shall administrate Policy control, Data Center control, user awareness, legal control, as well as performance estimation solution.

From the perspective of organizational control, the paper proposed an automated control framework that includes independent governing aiming to mediate between the user and the cloud provider. In addition, the governing body is meant to be obligated to ensure the security of cloud based data center, implementation of a secure policy & control, increase the user awareness about security methods deployed, handling the legal matters, resolution of disputes, evaluation of performance and providing practical solutions. A short representation of the suggested framework that uses security parameters to compute the threat index, so that the governing body could use it to accomplish their tasks and employ it in the implementation and planning of the security policy to keep the organization in control from the cloud computing privacy and security problems.

Unauthorized Access in the Cloud Computing Environment was detected by Rasim & Fargana in 2014, so they proposed a method to expose unauthorized access to the cloud infrastructure. Collaborative Filtering Algorithm constructed on the cloud model was used to build the process. By modeling the ordinary actions of cloud users in the form of a cloud models, and comparing them with each other by utilizing the cosine similarity method. After using the collaborative filtering method, the deviations from the normal behavior are evaluated. If the deviation values are higher than the

set limit, the user who was permitted to the system is evaluated as illegal, if not, he is evaluated as a real user.

The paper, proposed a collaborative filtering algorithm built upon the cloud model to be utilized to detect the masquerade attacks in the cloud infrastructure.

The paper pointed out that the model could aid in identifying similarities between the users on the basis of the cloud model. While utilizing the similarity measurement method based on the cloud model, it doesn't demand a strict comparison between different users' score value of operations.

MAIN FINDINGS OF THE LITERATURE REVIEW

In Cloud computing, Identity Management is regarded as a critical security obstacle to assure and manage safe usage in excess of multi-provider Inter-Cloud environments with allocated security mechanisms, communication infrastructures, policies and processes.

A lot of work on this particular issue was undertaken and found to be useful in providing a background on Identity Management in cloud computing and related issues. Some of this work was impractical (gave unpractical background basis about the subject). Others was practical by focusing on the frame of the research's undertaken. Methods followed by the

researchers were covered and highlighted to show the major issues that play a crucial role in delaying the advancement of the sector.

Some papers presented the major identity management challenges and threats in the Inter-cloud including, (David et al., 2011)

- (a) Inter-cloud resources' identification and naming,
- (b) Identity information Interoperability in the Intercloud,
- (c) Inter-cloud's life cycle identity management, and
- (d) interactions using single sign-on on the Inter-cloud.

Other papers talk about issue, of privacy and types of identity management methods utilized for protect the privacy summarizing other methods of Identity Management such as Microsoft Windows Card Space, Open ID, and PRIME (Privacy and identity management for Europe). They focused on its limitedness, like a main limitation of the Window Cardspace is using a single layer authentication method and another is using a third party authentication methods, and a major limitation of PRIME is that it needs the SPs and the user agents to use the PRIME middleware, and OpenID is usually endangered by phishing attacks as in many IDMs, phishing in OpenID is a major issue. Although the security token might not transmit passwords, the user might be tricked into accessing the phisher's website by

the attacker, and that website site may take any security token the user gave requesting data such as a credit card number. The user's password will not be acquired from the faked website, but the phisher might acquire other important information. However, handling cloud computing encounters many traffic and security problems that must be dealt with. One of the solutions to this problems is load balancing. RBAC provides such answer. Because of that, Access management and Identity management are executed by the use of this method.

While a lot of cloud deployments might be stand-alone, it is obvious that secure federated community clouds, i.e., inter-clouds, are needed. Therefore, there should be methods that allow flexible enforcement of authorization and authentication across federated environments for federated identity management (FIM). Studies on this matter aim to add protocol independent federated identity management to the Open Stack services. After showing a convincing secure cloud federation example, and demonstrating the conceptual design for protocol independent federated access, a detailed federated identity protocol sequence is presented.

Managing digital identities on cloud SP (SAML-Security Assertion Markup Language) which is an open standard protocol used to exchange authentication and authorization data between two different security domains. SAML is a secure based XML communication mechanism that

shares identities between multiple organizations and applications and has the ability to eliminate most passwords in the cloud and enables SSO.

Some researchers suggested an approach that does not depend on a third party, and provides a minimum amount of data to the Service Provider, and gives the capability to utilize identity data on hosts that are not trusted.

Another approach suggested by some researchers secures the identity management, and to be appeared powerful way to secure your authorization and access management by making it safe to provide a secured cloud data management environment.

One suggested approach includes the use of the FCFS and RBAC technique hybrid. RBAC gives roles to clients with certain roles who could access only a certain document. Therefore, using this technique eases access management and identity management.

CHAPTER 3

IDENTITY MANAGEMENT CHALLENGES, THREATS AND AVAILABLE SOLUTIONS

3.1 CLOUD COMPUTATION CHALLENGE AND THREATS:

Cloud computation consists of three parties: Cloud user (Customer), Cloud Network and cloud Service Provider (CSP). And many security challenges faced at different levels and threats, like challenges and threats at user/host level, network Level and Cloud Service Provider level. These challenges and threats must be dealt with since it is necessary to keep the cloud up and running continuously (Umme et al., 2014):

1. **Least Privileges:** Least Privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily this principle limits the damage that can result from an accident or error (Jeff, 2003).

Privilege access Management constitutes one of the major identity challenges beside traditional logging and audit requirements, access privilege wants to be a judgment mechanism also. while, nearly all of the enterprise applications suffer from roles mismanagement, and the infringement of isolation of duties, thus the reporting for failure or success actions on this side is critical (Umme et al., 2014).

Threats: Attacks on connect to the network or identity services, like hogging resources or DDoS attacks, may degrade the performance or risk availability of an Identity management system. If there was a need for high availability or performance, you should consider redundancy and failover options.

2. **Openness:** Because Management is still developing, and therefore, developing a well-established standards is not yet, leading to issues such as lack of openness and vendor lock-in. Openness is critical, so it may be put converters in the future to be developed to ensure scalability and interoperability. Moreover, in view of the fact that identity information can be accessed by malicious or unauthorized intruders/users (Umme et al., 2014).

Threats: Acceptable security (monitoring, authentication access control, encryption, etc.) mechanisms are needed to take place for administration interfaces and accessing identity; else, unauthorized access over the network (eavesdrop) will be a major risk factor.

3. **Identity theft :** Cloud IDMS have to subscribe to the rule of least privileges and continue to use the workflow for more approved mechanism. However, since less privilege not involves only fixed resources and roles, but also the statement of the complex, and changes (technical and non-technical). Several of the Cloud IDMS Distributed operations today effective access

rights dramatically over even provided users who don't require access those rights (Umme et al., 2014).

Threats: Excessive rights to use provisioning conduct a lot of critical security issues containing identity theft, accidental access, unauthorized disclosure, and fraud.

4. **Availability, Confidentiality:** The goal of availability for cloud computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place, Confidentiality It means keeping users' data secret in the cloud systems (Santosh & Goudar, 2012). Cloud can be accessed through several applications and devices when increase the number of access points.

Threats:

Unauthorized disclosure, The threat of not have permission admission of identity credentials from strangers and employees (intruders/users) (Umme et al., 2014).

5. **Trust Management :** Trust management between the subscriber and Cloud identity provider will be one of the critical points that today's Cloud Identity Management systems must be handled.

Threats: confidence is a personal term and context-sensitive term which is making it very difficult to choose a Cloud identity provider with trusted identity services.

6. **Integrity:** Data integrity In the cloud system means to preserve information integrity (Santosh & Goudar, 2012). Integrity of information stored in the Cloud and identity data needs great and immediate attention.

Threats: Identity data and information lost or stolen (Umme et al., 2014).

In general, IDMSs are vulnerable to different performance and security bottlenecks, that limit their common adoption as a possible solution for secure, trusted, protected and dynamic Cloud environments.

3.2 IDENTITY MANAGEMENT CHALLENGES AND THREATS

Identity management in an enterprise is a collection of technologies and processes to secure and manage access to the resources and information of an organization and also to protect profiles of users which include information of customers. The evolution of the emergence of the Intercloud notion and cloud computation bring up many identity management challenges as in table (1).

3.2.1 INTERCLOUD RESOURCES IDENTIFICATION AND NAMING

Various types of shared resources in the cloud computation model puts the infrastructure of cloud computation users want to make sure the identity of the request resources is available and valid as it assigns the resource they want to ask.

Threats:

1. Univocality of resources' identity and unambiguous requests.

There is a strong need for suitable identification and naming mechanisms to enable permits unambiguous requests and univocality of resources identity.

2. Continuous need for updating of documents

There is a need for document to keep up to date with respect associated service attribute.

3.2.2 IDENTITY INFORMATION INTEROPERABILITY IN THE INTERCLOUD

Outsourcing internal services is a major reason for the enterprise to use the cloud computation model. Some organizations like adoption of this model because of the cost effective they practice, while they go through outsourcing. The services and applications inside a company are not separate, and usually they form a network of dependencies, among composite relations between them; few of this services might not be outsourced. So, it should be given special attention on interoperability.

Threats:

1. Use of language:

Use of different languages (like SAML assertions, X.509 certificates, or Web Service Federation security tokens) to express their identity information is a problem related to identity management systems interoperability.

2. Interoperability problems (Syntactic and Semantic obstacles):

Traditional identity management systems interoperability problems appears in the Intercloud and might be classified as semantic and syntactic, the two aspects must be solved by a full solution, that must be standard based. There is a syntactic obstacle that a full solution has to deal with. A Semantic obstacle appear if the parties agree at the syntactic level, use different

formats, meanings and names for identity attributes also cause incompatibilities. This problem presents a semantic obstacle that must be resolved also. But this syntactic level problems are solved by using translation mechanisms, and encapsulation.

3. Limitation of initiatives:

Initiatives are not enough in the Intercloud, so it need solutions with many kinds of services, subjects and resources.

4. Common services related with identity management

Few of services are available by companies IT departments inside companies that associated to identity management, like user provisioning, privilege management, access control and authentication. So solutions of identity management for Intercloud have to be compatible with existing systems of identity management in the establishment to help go for outsourcing of such advanced services.

3.2.3 INTER-CLOUD'S LIFE CYCLE IDENTITY MANAGEMENT

During the life cycle of an entity's digital identity, various changes concerning provision, attributes, entitlement, or authorization may be happened depend on an organization's policy and entity's behavior or availability. A quick Synchronization of these changes, to all involves parties inside the Intercloud, appears to be imperative to assure that every entity has the same confrontation.

Threats:

Synchronization delays

Synchronization delays could lead to security vulnerabilities and weakness resource sharing.

3.2.4 INTERACTIONS OF SINGLE SIGN-ON IN THE INTERCLOUD

With intercloud increasing numbers of potential interactions that can happen between various users involved in the data. In such interactions, the parties have to concern about exchange identity information, authentication and identification purposes, in spite of, the existence of preceding knowledge of each other's own identity information or not.

a) Users responsibility

From the perspective of identity management, the main actors involved in these interactions are:

1. Users of Inter-cloud, the users that request services and resources, like cloud providers, human users, internal applications or external applications.
2. Service Providers of Intercloud, providers of cloud that provide resources or services to the Intercloud users .
3. Identity Providers of Intercloud, providers of cloud that authenticate users of Intercloud share the authentication result to service providers of Intercloud. Also providers are responsible for managing, certifying, and issuing the identity information for their users within Intercloud.

b) Cloud Service Users threats

1. **Ambiguous responsibility:** Cloud service users made resources delivery among service models. Consequently, the IT system built based on customer services. The deficiency of a clear responsibility definition between cloud service Providers and users may raise conceptual conflicts. Every contradiction contractual services provided lead to anomalies and accidents or anomalies. however the problem of knowing which entity is the data controller (data processor stays open at an international scale).
2. **Loss of judgment:** The institution, part of the deportation of its own information system to cloud infrastructure means given control to the cloud service providers. This loss of judgment related to the models of cloud service.

- 3. Lost of confidence :** It is not easy for a user of cloud service to know the trust level of his provider because of unknown property of the cloud service. There are no measures of how to access and share the security provider's level formally. Also, the users of cloud services don't have the ability to estimate the level of implementation of the protection that the provider accomplished. This deficiency in the level of security due to the sharing of the provider of the cloud service constitutes a real danger to the security of the users of cloud services.
- 4. Service Provider Lock in:** As a result of the loss of judgment one expects a deficiency of choices on how to vary a cloud provider by other one. This is what happened if a cloud provider based on non-standard hypervisors or practical machine image format, and does not present tools to change practical machines to a standardized format.
- 5. Unsecure User Access of Cloud Service:** Hence the majority of the deliveries of recourses are done using remote connectivity, non protected APIs, majorly PaaS services and management APIs, is one of the easiest attack vectors. Methods of attack like exploitation of software vulnerabilities, fraud, and phishing still obtains the required outcomes. And most times re-use the credentials and passwords, increases the effect of those attacks. Cloud services add another danger to the users. If a hacker attains your account's credentials, they could monitor your activities and

transactions, redirect your clients to illegitimate sites, falsify data, and return falsified information. Your service or account instances can be the attacker's new base. Then, they might use the strength of your reputation to start a series of attacks.

6. **Deficiency of information/Asset Management** : When ready for using Services of Cloud Computation, user must take care about the deficiency of Asset/information management by cloud service providers like location of sensitive asset/information, lack of physical control for data storage, reliability of data backup, countermeasures for disaster Recovery, reliability of data backup.
7. **Data leakages and lost**: A serious problem to the users of cloud service happened when Encryption key or privileged access had been lost. Therefore, shortage of encryption management information like access privilege, authentication codes and encryption keys leads to data loss and unexpected leakage.

c) **Cloud Service Providers Threats**

1. **Ambiguous responsibility**: The roles of different users may be applied and defined in a cloud system, like cloud service provider/user, client supervisor of information technology, owner of data. Variation of user responsibilities and roles definition according to data ownership, maintenance of infrastructure, access control and other may induce business or legal discord.

2. **Protection Contradiction:** Cloud infrastructure is decentralized structure, so its protection mechanism is able to be contradiction between distributed security modules.
3. **Evolution Risks:** Once conceptual, enhancement of cloud computation is to suspension of a few options from the design stage to the implementation stage, some dependent software components of a system might be selected and implemented, while the system executes. The methodology of conventional risk assessment is no longer consistent with such an evolution. The system that assume safe during the design phase may feat vulnerability during its implementation because of the components of the programs implemented recently.
4. **Business Interruption:** The “as a service” feature of cloud computation allocate resources and offers them as a service. Cloud infrastructure all along with its business workflows thus depends on a wide range of services, from the application to the hardware. But, the disruption to the provision of services, like delay or black out, likely cause an intensive impact belong to the availability.
5. **Supplier Lock-in:** Service provider platform has been building using a component of hardware and software by providers. Some provider-dependent modules or workflows were implemented for functionality extension or integration. Because of the deficiency of standard Applications

Programming Interfaces, the chance to set out to another providers is not clear. As a result of the provider locked there might be a deficiency of freedom according to how to change a provider.

6. **License Risks:** License of software is generally based on the users' numbers or installations' numbers. Since creation of virtual machine will be used some times, the supplier might- have to get from a lot of licenses than mostly needed at a particular period. The deficiency of a cloud license management plan that only allows for payment to get used licenses might cause conflicts using the software.
7. **Regulation Conflicts:** According to the regulations of procedures of the host country, data might be protected by a different jurisdiction. International cloud service provider likely follow up the executive regulations of local data centers, that form the legal threat to be taken on consideration.
8. **Bad Integration:** Depart to the cloud is supposed transfer of a lot of data and main configuration changes (for example, network addressing). Depart of a part of the information technology infrastructure to an outside cloud service provider include deep changes in the design of infrastructure (such as security policies and network). A bad integration come out from inconsistent policy enforcement or incompatible interfaces might brought up impacts either non functional and functional effects.

9. Unsecure Administration Applications Programming Interfaces (API):

The administration middle-ware existing between the cloud service user and the cloud infrastructure may be unsure with not enough attentions to sanitation of cloud service user authentication and inputs. Non protected Applications Programming Interfaces, usually administration APIs is preferred to an attackers target. It is not limited to cloud environment. On the other side, the service-oriented approach makes Applications Programming Interfaces essential building block for a cloud infrastructure. Protecting them become the main concern for the security of the cloud.

10. Shared Environment: Cloud resources were virtualized, different cloud service users (competitors) share the same infrastructure. One main issue is caused by fragmentation of the data structure, data segregation, and resource isolation. Any violent and un-authorized access to cloud service user's private data can threaten the confidentiality and integrity.

11. Hypervisor Isolation Failure : The hypervisor technology is viewed as the cloud infrastructure basis. Multi virtual machines connected on a physical server sharing memory and CPU resources that the hypervisor virtualizes. The failure of mechanisms isolating attacks is a threat that could be launched on a hypervisor to get un-authorized access to the memory of other virtual machines.

- 12. Service Unavailability:** Availability is not specific to cloud environment. Since the principle of the service-oriented design, service delivery might be affected, while the cloud infrastructure is not available. Also, the dynamic dependence of cloud computation offers much more possibilities for attackers. A classic Denial of Service attack on one service might block all cloud system.
- 13. Data Unreliability:** The Data protection gives confidentiality as well as integrity to the data by embedding access to it. Users of cloud services are concerned about the way providers deal with their data, and if data is illegally altered or disclosed. Even if the trust of the user of cloud services isn't in the cloud security's central, it is a big marketing discriminator for the providers of cloud services to move forward in the process of migrating an IT system to a cloud environment.
- 14. Abuse of the Rights of Cloud Service Providers :** For a user of cloud services, the migration of a piece of its IT system to a cloud infrastructure implies provision of partial control to the provider. That constitutes a serious threat to the data of the users of cloud services, notably regarding privilege and role assignments of providers. In addition to the deficiency of transparency regarding the practices of cloud providers may lead to a malicious insider attack or a mis-configuration. Such security violations lowers the reputation of the provider, causing a lower trust of the cloud service user.

Table (1): Identity Management Challenge and threats

Challenge	Description	Threats
1) Intercloud resources Identification and Naming	Surplus types of shared resources in the cloud computation model puts the infrastructure of cloud computation users want to make sure the identity of the request resources as it should know for sure who is the one resource they want to ask.	<ol style="list-style-type: none"> 1. Univocality of resources' identity and unambiguous requests. 2. Problem of Continuous need for updating of documents
2) Identity information Interoperability in the Intercloud	Outsourcing internal services is a major reason for the enterprise to use the cloud computation model. Some organizations like to adopt this model because of the cost effective they practice while they go through out sourcing. The services and applications inside a company are not separate, and usually they form a network of dependencies, with compound relation between them; few of this services may not be outsourced. Then it should be given special attention on Interoperability.	<ol style="list-style-type: none"> 1. Use of language 2. The interoperability problems (Syntactic and Semantic obstacles) 3. Limitation of initiatives 4. Common services related with identity management

<p>3) Inter-cloud's life cycle identity management</p>	<p>During the life cycle of an entity's digital identity, various changes concerning provision, attributes, entitlement, or authorization may be happened depending on an organization's policy and entity's behavior or availability. A quick Synchronization of these changes, to all involves parties inside the Intercloud, appears to be imperative to assure that every entity has the same confrontation.</p>	<p>1. Synchronization delays</p>
<p>4) Interactions of Single sign-on in the Intercloud</p>	<p>With Intercloud increase the numbers of potential interactions that can happened between the various users involved in the data. In such interactions, the parties concerned to exchange identity information, authentication and identification purposes in spite of the existence of preceding knowledge of each others own identity information or not.</p>	<p>Threats for Cloud Service Users</p> <ol style="list-style-type: none"> 1. Ambiguous responsibility 2. Loss of judgment 3. Lost of confidence 4. Service Provider Lock-in 5. Unsecure User Access of Cloud Service 6. Deficiency of information/Asset Management 7. Data leakages and lost <p>Threats for Cloud Service Providers</p> <ol style="list-style-type: none"> 1. Ambiguous responsibility 2. Protection Contradiction

		<ol style="list-style-type: none"> 3. Evolution Risks 4. Business Interruption 5. Supplier Lock-in 6. License Risks 7. Regulation Conflicts 8. Shared Environment 9. Unsecure Administration (API) 10. Bad Integration 11. Hypervisor Isolation Failure 12. Service Unavailability 13. Data Unreliability 14. Abuse of the Rights of Cloud Service Providers
--	--	--

3.3 SOLUTIONS AVAILABLE TO MEET THE CHALLENGES AND THREATS IDM

Available solutions to the challenges IDM and threats shown in Table (2) are:

a) Intercloud resources Identification and Naming

The existing approach for identifying and naming Cloud resources was shown in (Celesti et al., 2010), on base on the use of Extensible Resource Identifier (XRI, 2015) and eXtensible Resource Descriptor Sequence" (XRDS, 2015). XRI is a resolution and scheme protocol for abstract identifiers in harmony with uniform resource identifiers (URI) (In computation, a uniform resource identifier is a set of Characters used to identify the resources names). This selection can affect the representation of resources on the network. While XRDS is an XML-based general layout for service discovery and resource description, XRDS enable the resources description, in addition to, their related services, these are named service endpoints (SEPs).

But, OASIS has lately issued Extensible Resource Descriptor (XRD) V1.0) (XRD, 2015), which is new standard for resources discovery and descriptions, it replace XRDS. The major difference between XRD and XRDS is while XRDS describes services related to a resource (*endpoints*) in a one document, XRD explains every endpoint in a separate document and

connects them each other and with everyone in the resource document. Thus, XRDS documents should to be reserved up to date with respect their related services attributes, this is controllable in private environments where all services, control is seized by the same administrator, but, it is not the case in Intercloud state, therefore it is necessary that every service described separately.

b) Interoperability of identity information in the Intercloud

With respect to issues of compatibility between different themes on the semantic level plans and standards such as ITU-T Recommendation X520 (X.520, 2008) and ITU-T Recommendation X521 (X.521, 2008), (Recommendation X520 defines a number of attributes types and matching rules that might be helpful for a variety of applications to lead single particular use for many of the specific features in the names formation, particularly for categories of objects specified in Recommendation ITU-T X521. There are other types of attributes and qualities and called on the notification, and provide diagnostic information that recommendation, identifies the international standards connection types that supply associated with the attribute values of properties, also includes definitions of sentences LDAP relevant to attribute types and rules of matching). and references 4519 (Request for Comments) 4524 and (Sciberras, 2006) (Zeilenga, 2006).

These initiatives are not enough in Intercloud; There is need for solutions that have additional kinds of services, resources, and subjects. The use of ontologies can tackle problems of interoperability (Wache et al., 2001) (Priebe, et al., 2006), that might make integration of heterogeneous attribute schemes possible.

c) Inter-cloud's life cycle identity management

In this direction, Service Provisioning Markup Language (SPML) proposed by OASIS, an XML framework for managing allocation and Provisioning of system resources and identity information inside and between organizations (SPML, 2003).

SPML Version-1 was built on the OASIS Directory Services Markup Language (DSML, 2015) Version-2 (an XML representation of the Lightweight Directory Access Protocol), it is expected to join a family of standards designed to ease the implementation of Web services, and to establish interoperability surrounded by provisioning systems that allow organizations to securely create end-user accounts for applications and Web services from a single point in an organization.

One SPML request message may be used to create user accounts at the

same time in a multi-provisioning systems. De-provisioning is done by closing access accounts for any employee leave a company. This excludes dead accounts and prevents ex-employees from gaining access to customer systems.

d) Interactions of Single sign-on in the Intercloud

In this direction, proposing an infrastructure for identity management capable of supporting authentication between the Federal clouds, based on the assertions SAML, in (Tusa et al., 2010) and Openid can solve this problem. Openid and SAML were discussed in next topic.

Table (2) : Available solutions for challenges and threats

challenge	description	Name of Products
Intercloud resources Identification and Naming	It is essential that each service is described independently, but this is not the case in the Intercloud environment.	<ul style="list-style-type: none"> • XRI • XRDS • XRD 1.0
Interoperability of identity information in the Intercloud	Traditional identity management systems Interoperability problems appears in the Intercloud.	<ul style="list-style-type: none"> • X.521 and X.520 ITU-T Recommendations • RFCs 4519 and 4524 (Request for Comments)

Inter-cloud's life cycle identity management	A quick Synchronization of changes happened during the life cycle of an entity's digital identity concerning provision, attributes, entitlement, or authorization, to all involves parties inside the Intercloud, appears to be imperative to assure that every entity has the same confrontation	<ul style="list-style-type: none"> • Service Provisioning Markup Language (SPML)
Interactions of Single sign-on in the Intercloud	The parties concerned with exchange identity information, authentication and identification purposes in spite of the existence of preceding knowledge of each other's own identity information or not.	<ul style="list-style-type: none"> • SAML • OpenID

3.4 STATE OF THE ART OF SOLUTIONS APPROACHES

This section present brief description for the Identity Management frameworks:

3.4.1 FRAMEWORK DEFINITION

A Framework is a conceptual or real structure created to act as a guide or support to create something that changes the structure to be useful. A framework is usually more prescriptive than a structure and more comprehensive than a protocol.

A framework is often a layered structure indicating how programs would interrelate, and what kind of them can be built in computer systems. Some

computer system frameworks provide programming tools for using the frameworks, specify programming interfaces, or include actual programs.

In computer programming, a software framework is a briefing in programs that provide public functions that can be selectively changed by additional code written by the user, hence giving software that is application specific. A software framework is reusable, universal, and can provide a range of functions as a part of a larger software environment software platform to simplify the development of software products, solutions, and applications. Software frameworks can have code libraries, support programs, tool sets, compilers, and Application Programming Interfaces (APIs) that enable development of a solution or a project by combining different components.

3.4.2 IDENTITY MANAGEMENT FRAMEWORKS

There are many Identity Management Frameworks as:

3.4.2.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML)

It is an open standard data format for exchange of authentication and authorization data between identity Provider and Service Provider via internet. (Lewis & Lewis, 2009). The Consortium for defining SAML standard and security is Organization for the Advancement of Structured Information Standards (OASIS) (Juraj et al., 2012) (Gopalakrishnan, 2009).

There are three versions of SAML: SAML1.0, SAML1.1 and the new major version of SAML is 2.0 became an official OASIS standard in March 2005.

The four Components of SAML are: (Juraj et al., 2012)

1. Assertions: SAML assertion is the transaction from the identity Provider to the Service Provider.
2. Protocols: Which are used to communicate assertions between the service provider and identity Provider.
3. Bindings: Which are used to Map the SAML Protocol on to lower level network communication Protocols which are used to transport the SAML assertion between the identity Provider and Service Provider.
4. Profiles: The highest level of SAML Component which use cases between identity Provider and Service Provider that indicate how assertion, Protocols and Bindings will work together to Provide single-sign-on.

The Identity Provider or the Service Provider can initiate the web browser Single-sign-on profile. If the Identity Provider initiates it, the assertion is either encrypted, signed, or both. Figure (2) shows the Identity Provider Initiated SAML, assertion Flowchart. In this:

- 1) A request is sent by the browser to an identity provider for access to resources.

- 2) Identity provider redirects with Authorize Request to Browser. Identity provider gets Authorize Request from Browser. The identity provider sends the challenge for credentials or proof to the Browser like username or password.
- 3) Browser login with username and password.
- 4) Identity provider response with signal in HTML form to Browser.
- 5) Browser POST SAML response to the Service Provider.
- 6) Service Provider checks authentication and authorization from SAML Assertion.
- 7) Service Provider supplies resources to the browser.

In the case of service provider initiated SAML Assertion flowchart, the user is redirected back to the identity provider's federation web page with a SAML request by the service provider.

SAML is a single login process so that you only log in once using your username and password and use many services and applications at once. So, the time spent by users to log into multiple platforms and applications is reduced. SAML also improves the effectiveness of all Networks. It also reduces the Administrative expenses. SAML does not require user information to be maintained and synchronized between databases. The limitations of SAML are single point of failure. It adds the cost and the necessary information disclosure between the trusting site and SSO authority.

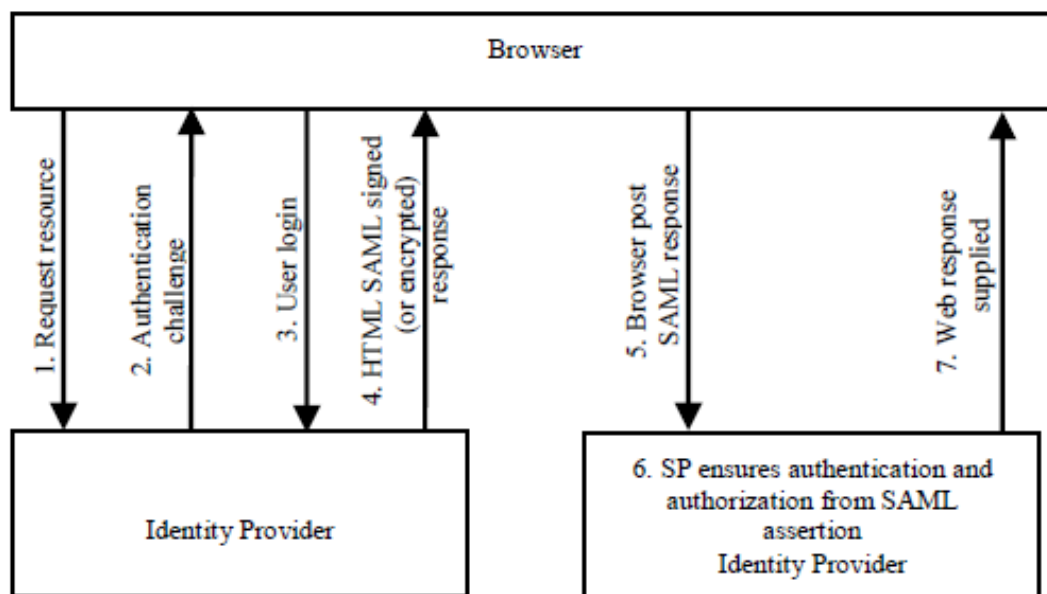


Figure (2) : Identity Provider Initiated SAML Assertion Flowchart

(Somorovsky et al., 2012)

3.4.2.2 LIBERTY ALLIANCE

Liberty Alliance defines sets of protocols which collectively offer solutions for identity federation management, cross-domain authentication and session management (Scott et al., 2004). Liberty Alliance Circle includes User, Service Provider (SP), and Identity Provider (IdP). It is the single-sign-on in which no need to authenticate again. Steps for single-sign-on being as given in figure (3)

- 1) User → SP: User request for services.
- 2) SP → User: Choose the Identity Provider, where the User federated his identity.

- 3) SP → User: SP acknowledges the IdP chosen and redirects the User to Identity Provider sites.
- 4) User → IdP: Authenticate the User against the Identity Provider and also contain the Information about the Service Provider.
- 5) IdP → User: Identity Provider generates SAML Token.
- 6) IdP → User: Send Response with the Token inside the message.
- 7) User → SP: Send the Token.
- 8) SP → IdP: Service Provider Communicate with Identity Provider for Verification of User Authentication.
- 9) IdP → SP: Identity Provider response with assertion to the SP.
- 10) SP → User: SP Provide the services to the user on the basis of Assertion.
- 11) SP → User: Response with the service.
- 12) SP ↔ User: Service Provider Provide the service to the User.

While the identity is proven by Authentication, another concept is used called Authorization. Authorization is used to grant access permissions for users with multiple levels. After finishing the Authentication, Authorization and Single Sign-On mechanism, Liberty Alliance specifications also include the Single Sign-Out mechanism.

The user sends request for single Logout to identity Provider. Identity Provider directing the request to Service Provider. Service Provider does

Process for Log out. Service Provider sends response to the Identity Provider. Identity Provider forward Single Log out confirmed to the user. The Liberty Alliance is Single-Sign-On and it authenticate and Authorize user Profiles. It also Provide the Scalability (Dwiputera & Ruppaa, 2012).

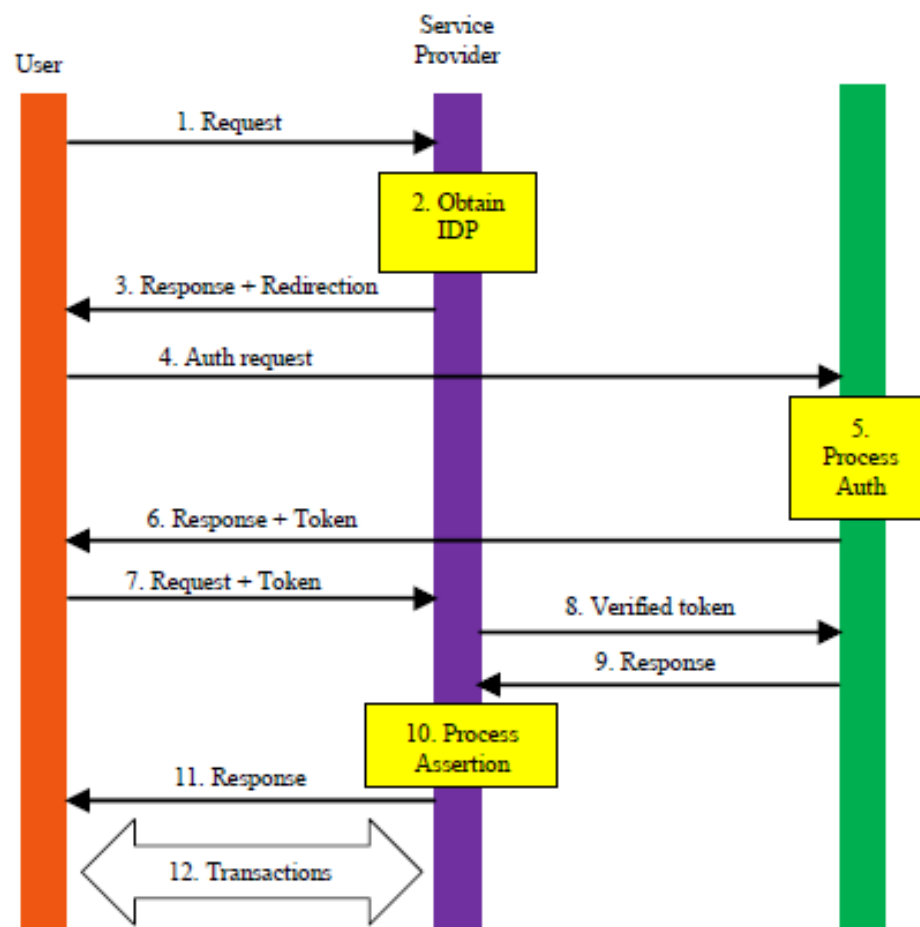


Figure (3): Single-Sign-On
(Dwiputera & Ruppaa, 2012)

3.4.2.3 WINDOWS CARDSPACE

Windows CardSpace is an Identity metasystem (system of systems) that gives a method, to manage a user's multi digital identities (Bhargava et al., 2011). It depends on the Concept of an Information Card based access platform/ architecture, developed for windows XP. A plug-in for Internet explorer 7 browser is used. Microsoft CardSpace is based on Web Service-Federation protocol which consists of the following specifications giving a base model for federation between Relying Parties and Identity Providers: WS-Security, WS-Security Policy, WS-Trust. Three parties are involved in this identity system:

- 1) Identity providers: Which supply digital identities (as trusted third-party).
- 2) Relying Parties: Identities are required to offer a services to users
- 3) Service requestor: Individuals and other entities related to whom claims are made.

The CardSpace identity metasystem makes use of XML based protocols, impeding the Simple Object Access Protocol (SOAP) and Web Services protocols). The message flows of the CardSpace framework are as follows. Here (see figure (4)) CardSpace-enabled User agent (CEUA), Relying Party (RP) and Identity Provider (IDP) are involved(Bhargava, B., et al., 2011).

- 1) CEUA → RP: HTTP receive Page Request to Login HTML.
- 2) RP → CEUA: HTML Login Page + InfoCard Tags (XHTML or HTML object tags).
- 3) RP ↔ CEUA: CEUA retrieves security policy via Web Service Security Policy.
- 4) User ↔ CEUA: User gets InfoCard.
- 5) IDP ↔ CEUA : Authentication of User.
- 6) IDP ↔ CEUA: CEUA retrieves security token via Web Service Metadata Exchange and Web Service Trust.
- 7) CEUA → RP: CEUA provide the security token via Web Service Trust.
- 8) RP → CEUA: Ok , logged in now.

The messages in steps 3, 5, 6, and 7 must be carried over Secure Sockets Layer/Transport Layer Security (SSL/TLS) channel to maintain confidentiality.

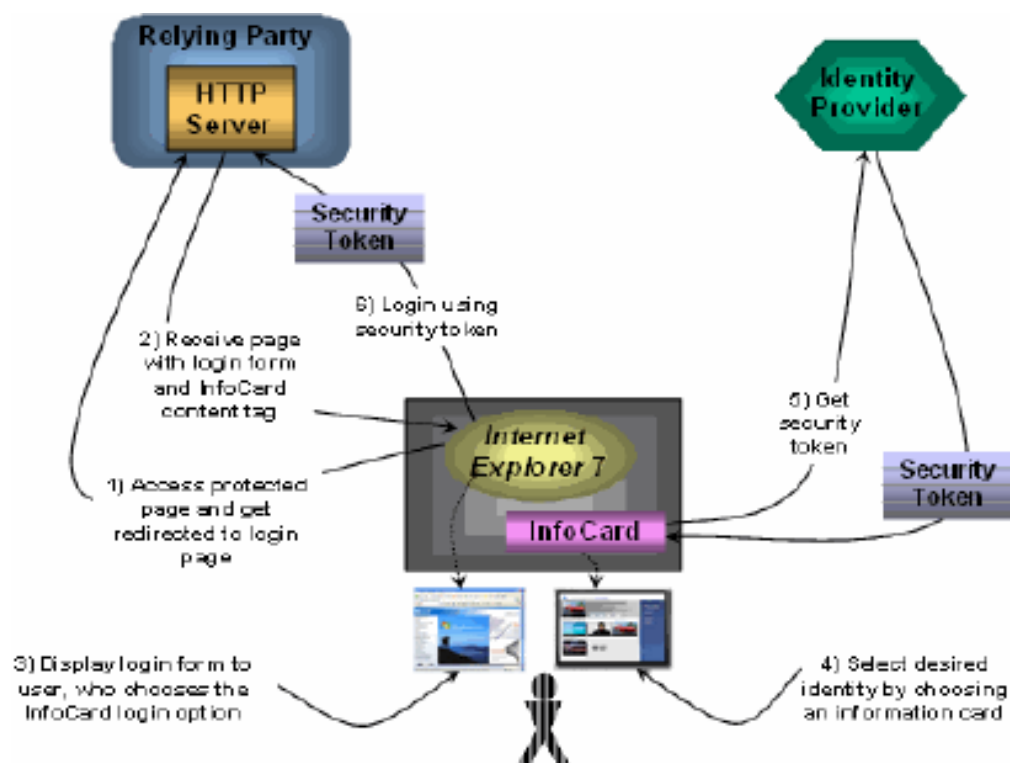


Figure (4): CardSpace Model of Identity Management
(Bhargava et al., 2011)

It is more flexible than user name and password. It employs strong cryptography, making it safer than password for use. It can potentially support any type of identity claim that it makes sense to all of the interacting parties and that users are ready to release. The CardSpace framework is criticized due to its reliance on the user's judgment of the confidence of an Relying Party. Many of them do not pay attention when asked to approve a digital certificate of an Relying Party, either because they know that they must approve the certificate in order to get access to a particular website or because they do not know the importance of the approval decision. Relying Parties with no certificate may be used in the CardSpace framework. In a

case where multiple Relying Parties and one Identity Provider are involved in a working session, the security identity meta system inside the session will depend on the authentication of the user to the Identity Provider only. In the case of the password is cracked or a working session is snatched the security of the entire system is threatened. To defeat the security imitation mentioned above use the Zero-Knowledge Proofing, Selective Disclosure, Anonymous Credential (Bhargava et al., 2011).

3.4.2.4 PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE (PRIME)

PRIME is a project for privacy architecture production, and a model and various application Scenarios (Camenisch et al., 2005). The three parties involved in PRIME are: User, Service Provider and Certification Authority. User requests for services or resources to service provider, and Service Provider provide the services as per user demand. Certification Authority is certifying authority (special type of service provider), which issued the certificates that are digitally signed statement. The PRIME involves four cryptographic tools namely secure communication, anonymous communication, pseudonyms, credentials and proofs of credentials ownership. Figure (5) present The execution of transactions.

PRIME is an User-controlled privacy-enhancing means that each individual user is put into control with respect to her/his Personally identifiable

information (PII) as possible. It is comprehensive means bringing diverse research areas (system architecture, cryptography, policies) and models together such as Designing and evaluating early models, learn some lessons how to integrate their achievements, and close the remaining gaps. It is a large scale means that system architecture, privacy and security mechanisms, terminology, prototypes, and tutorials are developed, evaluated and presented to the public. The Limitations of PRIME is that the product is not standardized and it is only possible unless it is interoperable with existing systems. It has its middleware which should be implemented on senders and receiver side console, which is an extra overhead (Camenisch et al., 2005).

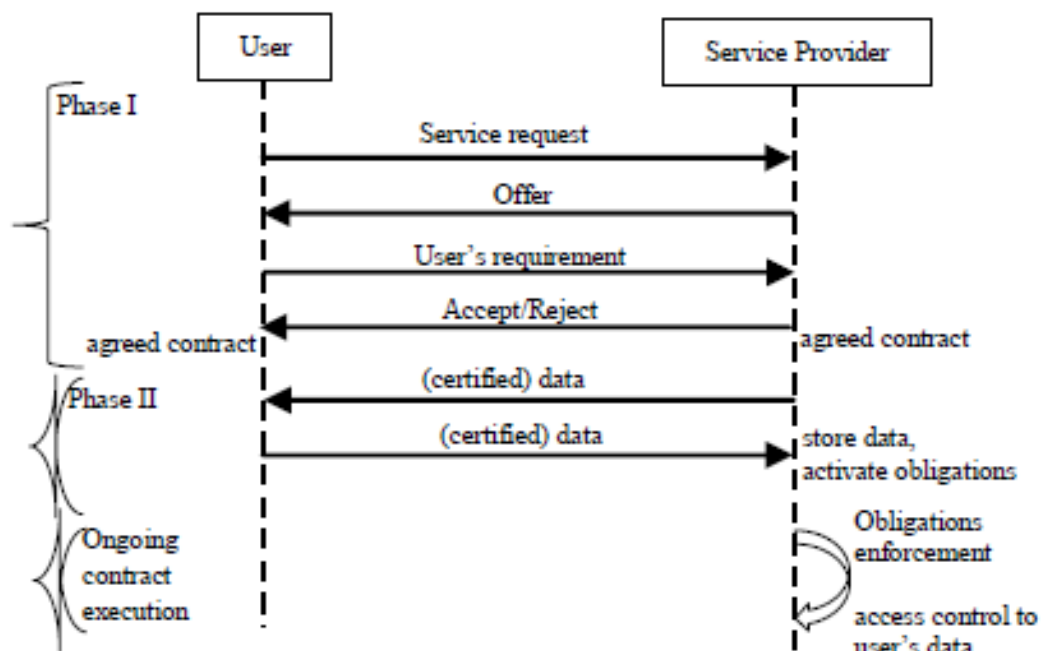


Figure (5): Execution of a transaction (Camenisch et al., 2005)

3.4.2.5 OPENID

OpenID is an easier way, faster, and safer way to log on to websites. OpenID is a non centralized model for identity management, that permits service providers to delegate the users authentication to identity provider. In this model, the user identity is represented by a Uniform Resource Locator (URL), called an OpenID identifier. Thus, users do not need to do an account for each site; but, they just use their OpenID identifier, and the authentication procedure will be conducted through the user's identity provider (David et al., 2012). The flow of OpenID as shown in figure(6) and listed below (David et al., 2012):

1. User sends requests for access to a service or resource at the Service Provider site.
2. Service Provider requires the user authentication and asks for his OpenID identifier.
3. User provides an OpenID identifier.
4. OpenID permits the user to easily provide the identifier of his identity provider, enhancing through this way his privacy by reducing the chances of being traced through his identifier.
5. Service Provider performs a discovery process using the supplied identifier to locate the Identity Provider of the user.

6. Service Provider and the Identity Provider perform an association process, to generate a shared secret through a Diffie Hellman key exchange.
7. Service provider builds an authentication request and redirects the user to the Identity Provider site through an HTTP redirection.
8. User gets authenticated by the Identity Provider.
9. Identity Provider builds an authentication response and includes an assertion for authentication result.
10. Identity Provider signs the request. User go back to the service provider site to continue with the authentication process.
11. Service Provider verifies the authentication response and reads the attribute values on it.
12. User gets authenticated at the service provider site and can have access to the requested service. This provides the control of sharing information and faster & easier registration login.

The limitations of OpenId are Phishing Attacks.

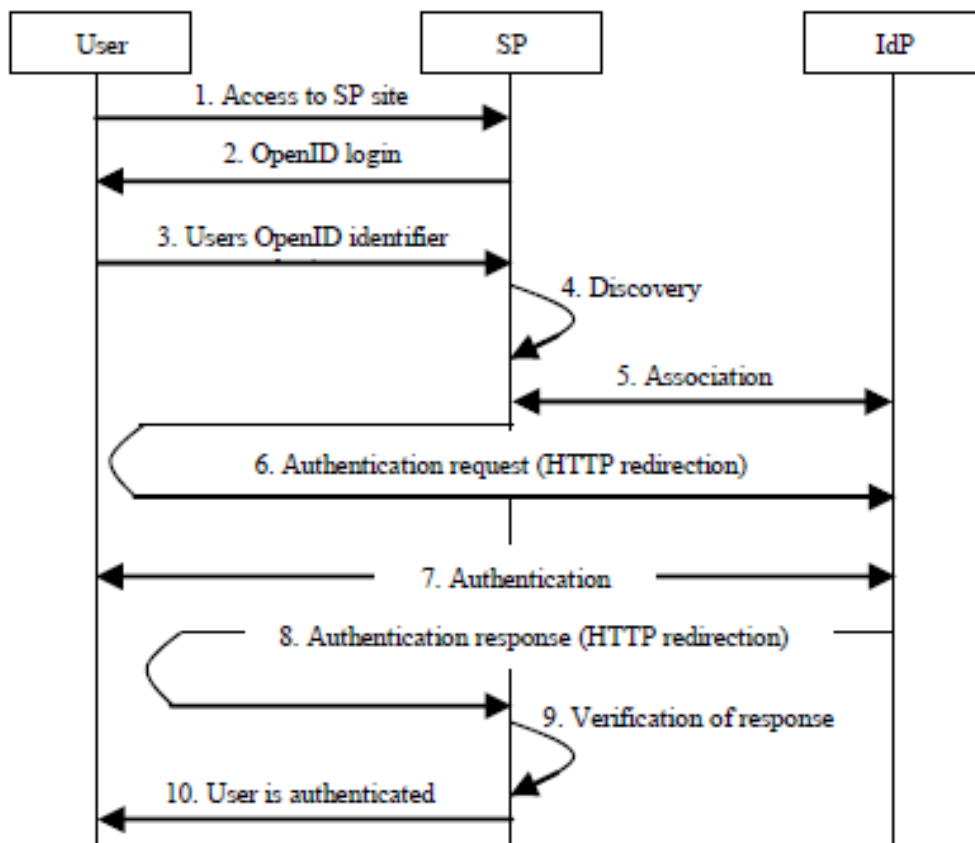


Figure (6): OpenID Authentication protocol (David et al., 2012)

3.4.2.6 OAUTH

OAuth is an Open Authentication method where user can share his stored resources to specific site with any other site instead of having to hand out her/his username and password (OAuth, 2007). It is flexible and designed to work with mobile devices and desktop applications. OAuth use Digital Signature, Hash Algorithm, Shared Secret, Nonce, Time Stamp. If the OAuth standard is extended by info cards support or other functionality in the future, it may be easily supported in any application. It is easy to manage or maintain configure to them. for example extranet login models with mixed authentication like SAML. It is Less data to store on servers.

3.4.2.7 ONELOGIN

OneLogin is the Single-Sign-On and Identity management for Cloud based Applications. It is good web applications for Saas. It is used to improve SaaS applications security, having a Centralized Password, user can get many secure password among his network of applications because he cannot remember all of them. OneLogin works by installing a browser extension that effectively pastes the credentials into the applications and logs user in. It supports the main Browser such as Chrome Firefox, Safari, and also supports the main windows OS's, Linux, Macintosh. Lightweight Directory Access Protocol and Active Directory , are available. It also supplies the De-Provisioning. OneLogin's Cloud identity platform comes ready for secure

single sign-on for mobile, iPad and web, federated search, user provisioning, deep directory integration with real-time user sync, out of band multiple factor authentication, A virtual private network integration and compliance reporting. OneLogin's catalog contains many thousands of pre-integrated applications, like Oracle CRM On-Demand, Salesforce.com, Microsoft Office 365, Google Apps, NetSuite, Innotas, LotusLive, Success Factors, WebEx, Workday, Yammer, Service Now (OneLogin, 2010).The

Advantages of OneLogin are :

- 1) Beautiful User experience
- 2) Simple to set up
- 3) Easy to use
- 4) Cross Platform and Cross Browser Support
- 5) Two factors authentication are available,
- 6) It is possible to add customer applications and any new applications.

Limitations of OneLogin are (OneLogin, 2010):

- 1) An application level only.
- 2) De-provisioning just prevent access to onelogin , don't lock or delete the application.
- 3) Don't do role on base on security.

3.4.2.8 WINDOWS IDENTITY FOUNDATION (WIF)

It is a Microsoft software framework for construction identity aware application . It is a framework for implementing claims on bases of identity in applications. The web services that use Windows Identity Foundation, the .NET frame work version 3.5 service provider(WIF, 2015)The

Characteristics of Windows Identity Foundation are as follows:

- 1) It provides templates which building claim-aware application.
- 2) It includes functionality that lets identities to be maintained across multiple service boundaries.
- 3) It includes a utility which help developers translate between NT tokens and claims.
- 4) It let developer to build claim-aware application by provide APIs.
- 5) It provides tools that helps developers to build custom security token services using ASP.NET.
- 6) It provide a ASP.NET controls which help developers to create web pages in claims-aware applications.
- 7) It provides utilities that create a trust relationship between a Security Token Service and Relying Party application.

The Claim-based identity involves Claim, Security Token, Security Token Service and Relying Party. Claim is identity information like email address, name, age. In Security Token the user delivers a set of claims

together with his request. In a Web service, this claims are carried in the security header of the SOAP packet. In a browser-based Web application, the claims arrive via an HTTP POST from the user's browser, and may later be cached in a cookie if a session is desired. They have to be serialized somehow, and this is where security tokens come in. It is a serialized set of claims that is digitally signed by the issuing authority. In security token service it is the plumbing that builds, signs, and issues security tokens according to the interoperability protocols. In Relying Party when you build an application that relies on claims.

3.5 REVIEW OF IDENTITY MANAGEMENT FRAMEWORK IN CLOUD

Table (3) presents Identity Management Frameworks and its Attributes and it contains comparison of different identity frameworks. It shows that all of them depends on Relying party/service provider initiated and there are limitations for some frameworks. It also suggests that in some of the identity frameworks, the registration and identity provider initiation are not required. Although most of the frameworks support single-sign-on, earlier identity frameworks were adopted by e-mail providers and corporate organizations use and government; currently they are extensively used in social networking sites and mobile apps.

Table (3): Identity Management Frameworks & it's Attributes
(Roshni et al., 2013)

Identi ty Fram ework	SAML	Libe rty Allia nce	Windows Cardspace	PRIM E	OPE NID	OAUT H	On eLo gin	Win dows Iden tity Foun datio n
Regist ration requir ed?	NO	Yes	Manifested through the installation of managed cards into the selection	Restri cted to registe red user	NO	Explicit identity services pre- register for a consum er key & secret	Yes	Yes
Protoc ols Used	SAM, XML, SOAP, HTTP	LDA P,X ML	XML based	Crypt ograp hi c protoc ols	XRD S, HTT P	JSON, HTTP	RD F,X .509	WS- Trust , WS- Secu rity, WS- Fede ratio n

limitat ions	The limitati ons of SAML are single point of failure. It added the cost and also the necessa ry informa tion disclosu re betwee n the trusting site and SSO authorit y	N/A	Major limitation of the Window Cardspace is relying on single layer authenticatio n and second is relying on the third party Another drawback is the judgment of the user in trusting the RP certificate and sometimes, in the CardSpace framework RPs with no certificates at all are used.	A major limitat ion of PRIME is that it requir es user agents and servic e provid ers to imple ment the PRIME middl eware	highl y at risk of phish ing attac ks.	N/A	N/A	N/A
-----------------	--	-----	--	---	---	-----	-----	-----

Identity provider initiated	Yes	Yes	NO	Yes	NO	Expected for OAuth V2.0	Yes	Yes
Main Purpose	Single-sign-on for enterprise users	Create an open network identity infrastructure	Single-sign-on for websites	For Data Minimization	Single-sign-on for Consumers	API authentication between applications	Single-Sign-On for Companies to secure access web application	Temporarily/ Disclosure of Credential or other Sensitive data

CHAPTER FOUR

THE PROPOSED IDM FRAMEWORK

4.1 PREFACE

This chapter will present the two concluded and main contributed part of this work based of comparative study of all related solutions so fare available and provided by researchers, organizations, authorities and leading concerned companies.

The first part will present in precise, simple, direct straight forward manner the general principles applied for selection a solution to the problem of IdM ,then by adaptation these principles suggest a general framework which will be the subject of the second part of the chapter.

4.2 PRINCIPLES OF SELECTION IDM FRAMEWORK:

The framework should be comprehensive composed of: a declared policy, the several bodies involved, the role of each body well defined, toggle scope and boundary of responsibility, components each with specified functions and control by governance independently body responsible for undertake to act as an interface between the beneficiary (organization and end user) and cloud computing service providers. The principles must satisfy the following conditions and requirements:

1. Framework Accommodate and adopt with continuous change in the cyberspace, virtual environment and its applications and services.

The system includes data protection incorporate:

- i. Identity establishing
- ii. Passwords system rules: ensure selecting hard-to- guess passwords. The difficulty of inferring seldom limitation passwords
- iii. Passwords Aging: changing passwords periodically and frequently.
- iv. Auditing as a means of monitoring potential threats.
- v. The verification and authentication mechanism
- vi. Resource Access Control
- vii. Data and Message security: ensure, Data integrity, confidentiality and origin authenticity)
- viii. Resources availability.

Identity establishing, Auditing verification and authentication Data integrity, confidentiality authenticity).

2. The framework includes the privacy protection measures of the user and his organization.
3. Four bodies mutually cooperates in establish identity during a session of one user accesses data required from Multi-provider cloud services integration. The four bodies as follow:

- i. The end user within the organization who enters by his personal traditional account to the network.
- ii. The organization of the end user, which take the responsibility of handles verification, authentication and linking personal account to the user with its reference and the user authorities matrix according to data and information policy declared by the Organization by the help of special application which is available from within the DBMS provider or from several organization companies an independent body.
- iii. Trusted independent authority responsible for governance, and preferably a formal, neutral body, which based on account descriptions attached to the user account sent by the Organization generating a special alternative account identity for each user valid only for one session used in to access all applications available by Multi p provider cloud services.
- iv. Cloud Providers : A cloud provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. Cloud providers are sometimes referred to as cloud service providers or CSPs.

4. Each services or access request consists of two parts, the first is the traditional user account information(both user name and password) and the other part is linked to by the organization the user belong to includes in addition to organization information a authority matrix and any necessary information.
5. The framework must protect of privacy of both the user and the organization.
6. The account, which is generated by governance body must be used once and for one user and during one session only and will not be used again, and for that purpose onetime pad key generation programs are recommended.
7. The key generated by the independent governance body is the base for control operations and the reference used by relevant authorities and for any finical and accounting stalemates.
8. Apart from the end user all other bodies are committed to share the log files of transactions and processes of each body per each individual user
9. The suitable methodology for implementation of the framework is service orientated architecture (SOA) due to the scalability, integration, evolutionary orientated of such design methodology.

4.3 THE PROPOSED FRAMEWORK

Taken in consideration the selection principles; the IdM framework proposed which including IdM management policy, bodies with multi level of authority and roles, components each with cretin functionality and procedures and organizational control framework consist technical, legal and policy control that ensure the right information at a right time provided for the right parties and grantee the security and privacy protection the proposed framework describe as follow:

4.3.1 THE FOUR BODIES INVOLVED IN FRAMEWORK

The four bodies involved in framework are:

- a) End user within the organization who enters by his personal traditional account to the network and request services.
- b) Organization, which is responsible for verification, authentication and linking personal account to the user with its reference and the user authorities matrix according to data and information policy declared by the Organization by the help of special application which is available from within the DBMS provider or from several organization companies an independent body.
- c) Governing Body which is Trusted independent authority responsible for governance, and preferably a formal, neutral body, which based on account descriptions attached to the user account sent by the

Organization generating a special alternative account identity for each user valid only for one session used in to access all applications available by multi provider cloud services.

- d) Cloud provider which is generally a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. Cloud providers are sometimes referred to as cloud service providers or CSPs. Bodies diagram is shown in figure (7).

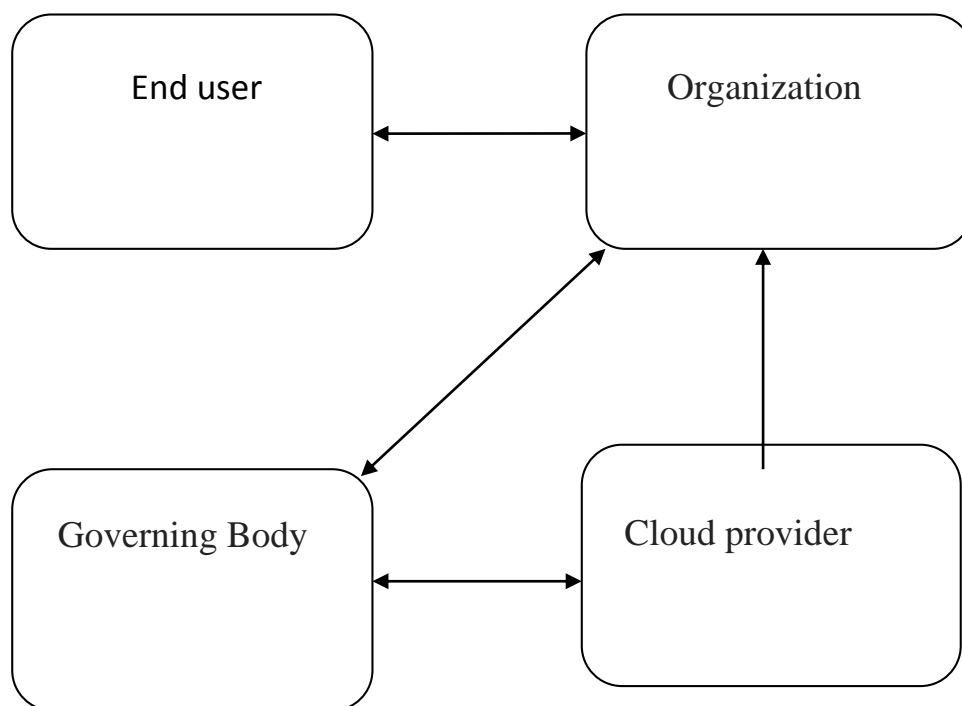


Figure (7): Conceptual framework proposed by the study.

Each one of the four bodies handles with responsibility of specific functions, table (4) present the role matrix of bodies involved in IdM proposed Framework.

Table (4): Roles Matrix of bodies involved in IdM Framework

function \ Body	Identity establishing	Auditing	Verification	Authentication	Integrity	Confidentiality	Privacy
End user	√	-	-	-	-	-	-
Organization	-	√	√	√	-	√	-
Governing Body	-	√	√	√	-	√	√
Cloud provider	-	√	-	-	√	√	-

4.3.1 ORGANIZATIONAL CONTROL FRAMEWORK

Organizational Control Framework consist of :

- a) Technical Control: Include user authentication (login), user name password, logical access controls, Auditing, Integrity, antivirus software, firewalls.
- b) Logical Control : Include policies, privacy laws, and clauses.
- c) Policy Control: Include Information Authority.

Figure (8) shows Organizational Control Framework.

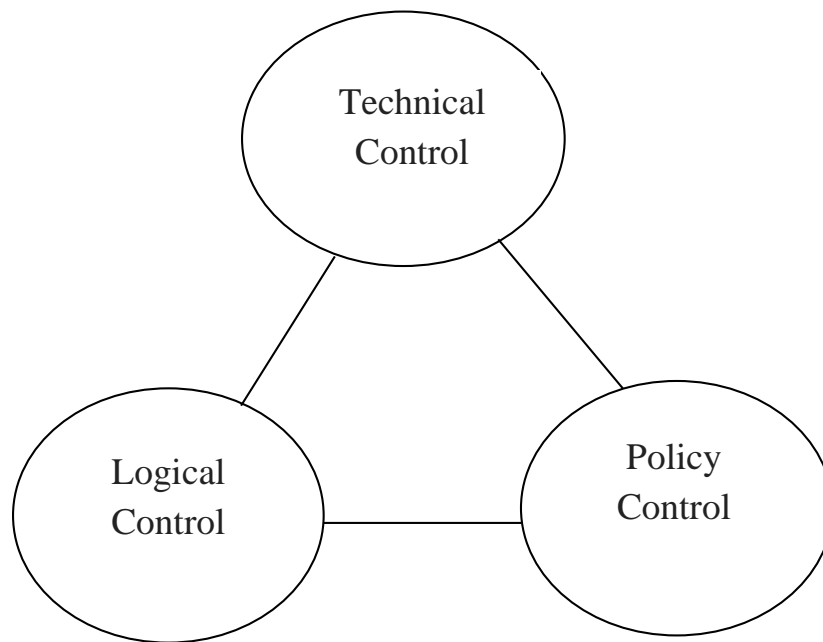


Figure (8) : Organizational Control Framework

4.3.3: ELEMENTS OF SECURE- CONTROL COMPONENTS

There are four elements of secure-control components :

- a) Identity establishment which is responsible for Creation of a new identity record, in an authoritative source, where none has existed previously.
- b) Resource Access Control which gives access to a computer system only to users who have the authorization to use a requested resource (such as a file, a printer queue, space to run a program, and so forth).
To do this, Resource Access Control Facility (RACF) identifies and authenticates a user, determines the resources to which the user is authorized, and logs and reports attempts to get access to protected resources by unauthorized users.

- c) Data and message Security includes Data Integrity, Confidentiality, origin authenticity.
- d) Resource Availability.

Figure (9.a) show Elements of Secure- Control components.

Elements of Secure- Control component
1. Identity establishment
2. Resource Access Control
3. Data and message Security (Data Integrity, Confidentiality, origin authenticity)
4. Resource Availability

Figure (9.a) : Elements of Secure- Control component

Elements of Secure- Control components shown in figure (9.b) when user want to login send request to authentication authority and to access control, authentication authority send approval to access control and then he can login by new password for one session.

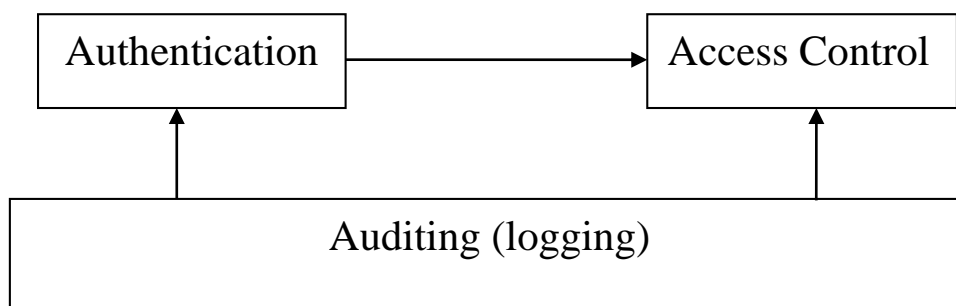


Figure (9.b): Functions of Secure-Control component

4.3.4 : PASSWORD SYNTAX RULES

The account, which is generated by governance body must be used once and for one user and during one session only and will not be used again. and for that purpose onetime pad key generation programs are recommended. Figure (10) show Password Syntax Rules

The key generated by the independent governance body is the base for control operations and the reference used by relevant authorities and for any finical and accounting stalemates.

Apart from the end user all other bodies are committed to share the log files of transactions.

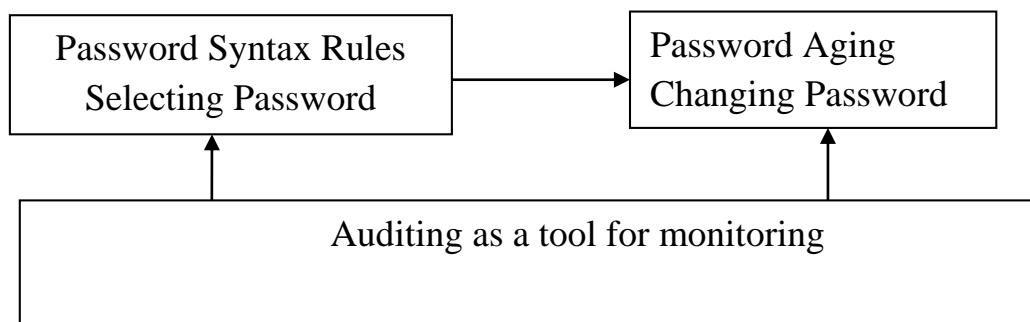


Figure (10): Password Syntax Rules

4.3.4 SCENARIO OF WORKING FRAMEWORK

Accommodate and adopt with continuous change in the cyberspace, virtual environment and its applications and services.

The proposed framework Circle includes User, organization ,Identity Provider and Service Provider, cloud provider . It is based on use username and password for one time only and it will be changed every time the user request services. Steps for this framework being as given in figure (11) and it operates as follows:

- 1) User Request for services by his personal account in the organization.
- 2) organization of end user handles verification, authentication and linking personal account to the user with its reference and the user authorities matrix according to data and information policy declared by the Organization by the help of special application which is available from within the DBMS provider or from several organization companies an independent body.
- 3) Trusted independent authority responsible for governance, and preferably a formal, neutral body, which based on account descriptions attached to the user account sent by the Organization generating a special alternative account identity for each user valid

only for one session used in to access all applications available by Multi p provider cloud services.

- 4) Access request consists of two parts, the first is the traditional user account information (both user name and password) and the other part is linked to by the organization the user belong to includes in addition to organization information authority matrix and any necessary information send to cloud provider.
- 5) The account, which is generated by governance body must be used once and for one user and during one session only and will not be used again(generate by pad key generation programs).
- 6) User get the service from cloud provider.

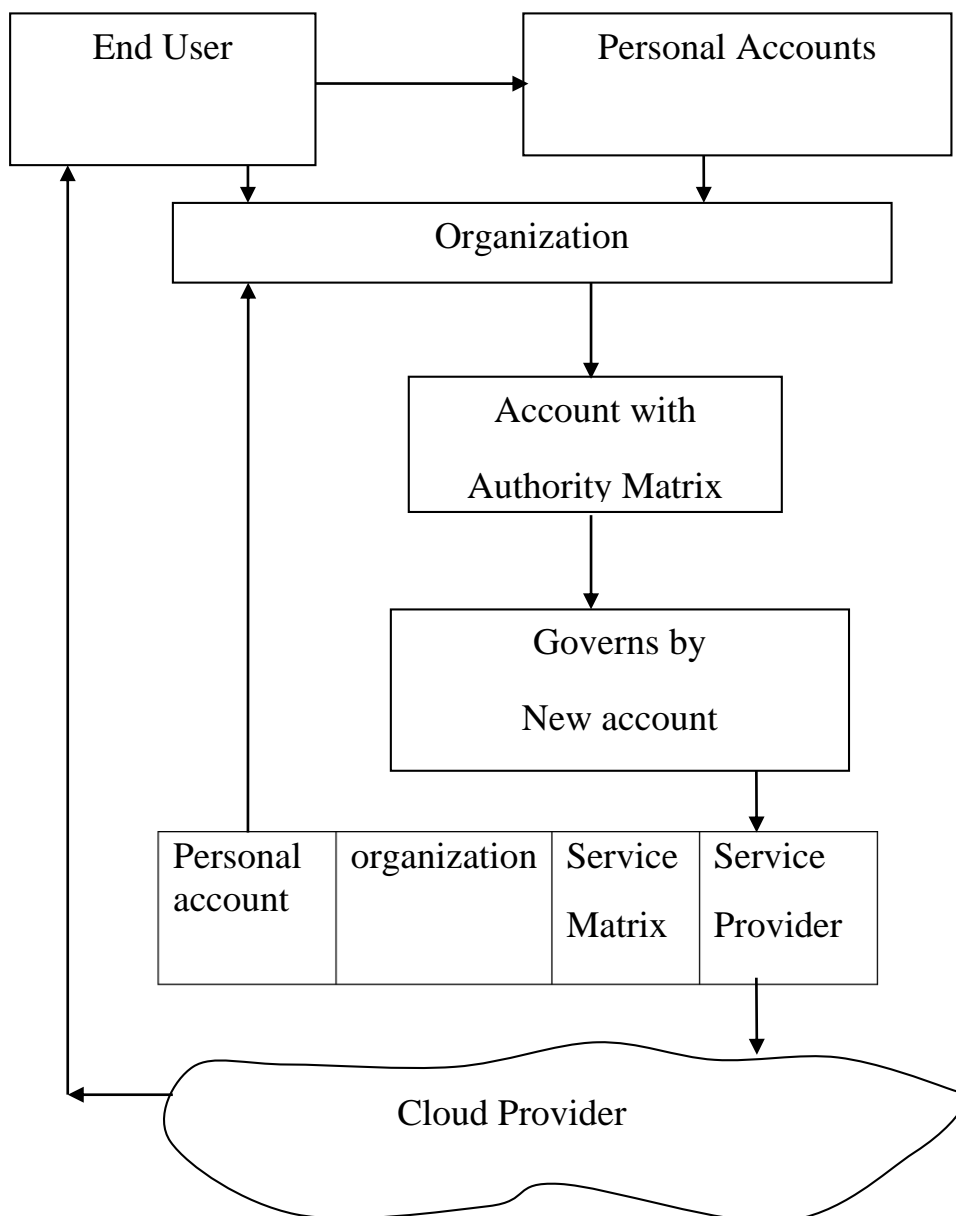


Figure (11) : Scenario of working framework

CHAPTER FIVE:

CONCLUSION AND RECOMMENDATIONS

5.1 CONCLUSION

In this thesis, the researcher has highlighted the major issues for identity management in open environments as cloud environment and inter cloud environment through the presentation of their definitions and major related subjects. It illustrates challenges and threats for cloud computation and intercloud environment challenges and available solutions.

5.1.1 GENERAL FINDINGS OF THE THESIS MAYBE SUMMARIZED AS FOLLOWS :

1. Number of users and resources for internet and inter cloud are increasing over time.
2. Security is critical issue to the intercloud environment, a fact that should be undertaken into consideration and put under focus during all stages since we are not just dealing with financial transactions that can be tackled through penalties in case there is a data breach. Here we are talking about systems with infiltration that could lead to loss of lives and/or cause massive disturbance to the society.

3. Privacy and security remain a high level threat in the management environment of cloud data, taking into account that the data's privacy is influenced as the users of cloud don't have full awareness about the data's location in servers.

5.1.2 IDENTITY MANAGEMENT FINDINGS

1. Users of cloud services can only access using the deployed services to access, modify, and remove their information, that are out sourced by them (whatever the private or public data) and these can only be accessed using deployed services.
2. Identity management issue is very important for the environment of cloud computing. The management of user credentials and remote access introduced concerns for privacy. Many ways to deal with the issue exist, but a few of those offered a simple and trust-based method for the service and application of cloud computing.
3. Most of previous solutions for identity management in intercloud environments still have limitations and shortfalls

Based on the above findings, the current thesis proposed a framework for identity management that takes into account limitations and shortfalls of previous frameworks that were in place with the purpose of identifying users and resources related to intercloud environment.

5.2 RECOMMENDATIONS

Based on the above, the following should be kept in mind regarding cloud computing, management and security:

- 1) Implies a better method to enhance the abilities substantially with no expenses spent in new infrastructure or licensing new software.
- 2) Despite the efficient use of resources by virtualization techniques and taking up a lot of the work load from the user, security risks fraught cloud computing, and this issued should be highly considered.
- 3) Usual identity management systems are designed to be cost effective and scalable mainly for the SPs, but not essentially for the users, and that often causes poor usability.
- 4) Pear in mind that any framework will have some limitations, it is expected that extensive future research will be of value as it may cover any gap areas in this regard.
- 5) Further research is appreciated and encouraged in particular fields such as identity management for open distributed environment.

At the end of this thesis, the research has the hope that the current thesis will help in covering a gap that is may existed and provoke problems to researchers in the subject. Further research is appreciated and encouraged in particular fields such as identity management for open distributed environment.

REFERENCES

- Adrian, B., Marco, M., Yolanta, B., and Simon, S. (2007). On Identity Assurance in the Presence of Federated Identity Management Systems. Retrieved from: <http://www.hpl.hp.com/techreports/2007/HPL-2007-47.pdf>
- Ajay, P., and Prasun, C. (2013). **Centralized Access Management and Monitoring as a Service in Cloud Environments-A Critical Study**. Computer and Information Science, 6(2).
- Amir, H., and Thomas, R. (2005). **Proposed Framework for an interoperable electronic IdM**. (Gartner. Gartner survey on consumer trust in online commerce 06/2005)
- Andrew, B., and Jeffrey, C. (2011). **Trusted Platform-as-a-Service: A Foundation for Trustworthy Cloud-Hosted Applications**, CCSW'11, October 21, 2011.
- Ardi, B. (2014). **An Identity Management Survey on Cloud Computing**, Int. Journal of Computing and Optimization, 1(2), 63–71.
- Audun, J., Mohammed, A. and Suriadi, S. (2007). **Usability and Privacy in Identity Management Architectures**, In the Australasian Information Security Workshop: Privacy Enhancing Technologies (AISW 2007).
- Bernstein, D., and Vij, D. (2010). **Intercloud Security Considerations**, 2nd IEEE International conference on Cloud Computing Technology and Science, pp. 537–544 (2010).
- Bhargava, B., Singh, N., and Sinclair, A., (2011). **Privacy in Cloud Computing Through Identity Management**. Technical Report. Computer Science, Purdue University.
- Bing, C., and Chengxiang, T. (2012). **RFID-based Electronic Identity Security Cloud Platform in Cyberspace**, journal of networks,7 (7).
- Camenisch, J., Shelat, A., Sommer, D., Fischer, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., and Tseng, J. (2005). **Privacy and identity management for everyone**. In Proceedings of the Workshop on Digital Identity Management.
- Cao, Y., and Yang, L. (2010). **A Survey of Identity Management Technology**. In Information Theory and Information Security (ICITIS), 2010 IEEE International Conference On, 287-293.

Celesti, A., Villari, M., Puliafito, A. (2010). **A naming system applied to a RESERVOIR cloud**. Sixth International Conference on Information Assurance and Security (2010).

Chang, S., Kuhn, R., Hu, C., and Polk, W. (2001). **Introduction to Public Key Technology and the Federal PKI**. National Institute of Standards and Technology.

Christian, E., Frank, B., Sebastian, K. and Sebastian, A. (2007). **Identity as a service-Towards a service oriented identity management architecture**. In: EUNICE'07 Proceedings of the 13th Open European Summer School and IFIP TC6.6 Conference on Dependable and Adaptable Networks and Services, pp. 1–8 (2007).

David, C., Kristy, S., Craig, L., Yann, F., and Damien, G. (2013). **Adding Federated Identity Management to OpenStack, J Grid Computing** (2014) 12:3–27

David, N., Agudo, I., and Lopez, J. (2012). **Integrating openid with proxy re-encryption to enhance privacy in Cloud-based identity services**. In Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom).

David, N., Isaac, A., Prokopios, D., and Stefanos, G. (2011). **Identity Management Challenges for Intercloud Applications**, 1st International Workshop on Security and Trust for Applications in Virtualized Environments (STAVE 2011) (2011). doi:10.1007/10.1007/978-3-642-22365-5 24.

David, N., Isaac, A., Prokopios, D., and Stefanos, G. (2011). **Identity Management Challenges for Intercloud Applications**, 1st International Workshop on Security and Trust for Applications in Virtualised Environments (STAVE 2011).

DSML (2015). **Directory Services Markup Language**, retrieved from <http://searchoracle.techtarget.com/definition/DSML>

Dwiputera, F., and Ruppia, S. (2012). **Single sign-on architecture in public networks (Liberty Alliance)**. In Proceedings of the INFOTECH seminar on advanced communication Services (ACS).

Elisa, B., Federica, P., Rodolfo, F., and Ning, S. (2009). **Privacy-preserving Digital Identity Management for Cloud Computing**.

FIDIS. (2008). Future of Identity in the Information Society, retrieved from, <http://www.fidis.net/>

Harshit, S., and Sathish, K. (2015). **Control Framework for Secure Cloud Computing**, Journal of Information Security, 6, 12-23. Available <http://dx.doi.org/10.4236/jis.2015.61002>
<http://dx.doi.org/10.4236/jis.2014.52007>
<http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.520>

Janaki, M., and Durga, M. (2013). **A Survey on Privacy Enhancement in Cloud Computing using Identity Management**. IJCSN International Journal of Computer Science and Network, 2 (6).

Jeff, L. (2003). **Implementing Least Privilege at your Enterprise**, SANS Institute, As part of the Information Security Reading Room.

Jensen, M. (2012). **On breaking SAML: Be whoever you want to be**, In WOOT, 2012.

John, R., Chris, S., Jim, W., and Andrew, W., Eds. **Reproduction for academic**, not-for profit purposes permitted provided this text is included.

Juraj, S., Mayer, A., Worth, A., Schwenk, J., Kampmann, M., and Kari, H. (2009). **OpenID and identity management in consumer services on the Internet**, TKK T-110.5190 Seminar on Internetworking 2009-04-27, Helsinki University of Technology.

Kerberos. (2015). **The Network Authentication Protocol**, retrieved from, <http://web.mit.edu/kerberos/>

LAP. (2006). **Liberty Alliance Project**, retrieved from, www.projectliberty.org

Lewis, K., and Lewis, J. (2009). **Web single sign-on authentication using SAML**, International Journal of Computer Science Issues, 2009, Vol. 2, pp. 41-48

Libor, S. (2012). **Cloud Computing: An Overview**. JOURNAL OF SYSTEMS INTEGRATION, 2012/4

Massimiliano, R., Hamza, G., Massimo, F., Neeraj, S., Jesus, L., Silviu, P., and Dana, P. (2012). **Security Issues in Cloud Federations, Chapter 10 in Achieving Federated and Self-Manageable Cloud Infrastructures**.

Theory and Practice, IGI-Global (2012). doi:10.4018/978-1-4666-1631-8.ch010.

Mauro, J., and Zair, A. (2012). **a study of access control in cloud computing environment.** *Research International Journal of Computers & Technology*, 3 (3).

Naqvi, S., Villari, M., Latanicki, J., Massonet, P. (2009). **From Grids to Clouds—Shift in Security Services Architecture**, CGW'09—Cracow Grid Workshop. Krakow, Poland. (2009)

OAuth. (2007). **Hueniverse Beginner's Guide to OAuth.** Available: <http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-ii-protocol-workflow>

OneLogin. (2010). Available: <http://www.justinpirie.com/2010/03/one-login-saas-app-review-1-the-good-bad-and-ugly>.

Pelin, A., Bharat, B., Rohit, R., Noopur, L., and Mark, L. (2010). **An Entity-centric Approach for Privacy and Identity Management in Cloud Computing**, Reliable Distributed Systems, *2010 29th IEEE Symposium on*

Peter, M., and Timothy, G., (2011). **The NIST Definition of Cloud Computing (Draft)**, Special Publication 800-145 (Draft). Recommendations of the National Institute of Standards and Technology. U.S. Department of commerce. January 2011.

PICOS. (2015). **Privacy and Identity Management for Community Services**, retrieved from , <http://www.picos-project.eu/>

Prasanalakshmi, B., and Kannammal, A. (2012). **Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics**, *International Journal of Computer Applications* , 53(18).

Priebe, T., Dobmeier, W., and Kamprath, N. (2006). **Supporting Attribute-based Access Control with Ontologies.** In: Proceedings of the First International Conference on Availability, Reliability and Security. IEEE Computer Society, Washington, USA, 465-472 (2006).

Ramkinker, S., Vipram, G., and Mohan, K. (2013). **Dynamic Federation in Identity Management for Securing and Sharing Personal Health Records in a Patientcentric Model in Cloud**. *International Journal of Engineering and Technology*, 5 (3).

Rasim, A., and Fargana, A., (2014). Illegal Access Detection in the Cloud Computing Environment, *Journal of Information Security*, 2014, 5, 65-71. Available <http://www.scirp.org/journal/jis>

Rizwana, S., and Sasikumar, M. (2013). **Identity Management in Cloud Computing**, *International Journal of Computer Applications* 63(11).

Roshni, B., Upendra, B., and Dhiren, P. (2013). **Identity Management Frameworks for Cloud**. *International Journal of Computer Applications*, 83(12).

Ruhi, G. (2014). **Implementation of an Efficient RBAC Technique of Cloud Computing in .Net Environment**. *International Journal of Computer Trends and Technology*, 8(3).

Santosh, K., and Goudar, R. (2012). **Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey**, *International Journal of Future Computer and Communication*, 1(4), December 2012.

Sarah, S., Muhammad, A., and Qaisar, J. (2013). **Evaluating Cloud Computing for Futuristic Development**. *International Journal of Computer Applications*, 61(6).

Sciberras, A. (2006). **RFC 4519 – Lightweight Directory Access Protocol (LDAP): Schema for User Applications**. Internet Engineering Task Force (2006).

Scott, C., John, K., and Darryl, C. (2004). **Liberty ID-FF Bindings and Profiles Specification Version: 1.2-errata-v2.0** found in <http://www.projectliberty.org/liberty/content/download/319/2369/file/draft-liberty-idff-bindings-profiles-1.2-errata-v2.0.pdf>.

Shibboleth. (2015). retrieved from , <http://shibboleth.internet2.edu/>

Simon, T., and Stuart, G. (2014). **Virtualization Security, Strategy and Management**, *Network and System Sciences*, 7, 423-429. Available <http://www.scirp.org/journal/ijcns>

Smita, S., and Deep, M. (2014). **Identity Management issues in Cloud Computing**. International Journal of Computer Trends and Technology , 9(8).

SPML. (2003). **Service Provisioning Markup Language**, Available: <http://xml.coverpages.org/ni2003-06-05-a.html>

Tewfiq, M., and Jean, S. (2007). **A Survey of "User-centric Identity Management Technologies**. In: International Conference on Emerging Security Information, Systems and Technologies, 12-17 .

Tusa, F., Celesti, A., Villari, M., and Puliafito, A. (2010). **Security and Cloud Computing: InterCloud Identity Management Infrastructure**. In: 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 263-265 (2010).

Umme, H., Rahat, M., Muhammad, S., and Muaz, N. (2014). **Cloud identity management security issues & solutions: a taxonomy**, retrieved from <http://www.casmodeling.com/content/2/1/5>.

Ushadevi, R., and Rajamani, V. (2013). **Real-Time Service Composition and Deployment for Secure Computing in Cloud Environment**. International Journal of Enhanced Research in Science Technology & Engineering, 2(4) , 91-99.

Wache, H., Voegelé, T., Visser, U., Stuckenschmidt, H., Schuster, G., Neumann, H., and Hübner, S. (2001). **Ontology-based integration of information-a survey of existing approaches**. IJCAI-01 workshop: ontologies and information sharing, 108-117 (2001).

WIF. (2015). **Windows Identity Foundation**. Available: <https://msdn.microsoft.com/en-us/library/ee517276.aspx>

WS-Federation. (2015). **Web Services Federation**, retrieved from, <http://www.ibm.com/developerworks/library/specification/ws-fed> (2007)

X.520. (2008). **ITU-T Recommendation X.520 (11/2008)**: The Directory - Selected attribute types (2008), available:

X.521. (2008). **ITU-T Recommendation X.521 (11/2008)**: The Directory - Selected object classes (2008), available: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9599&lang=en>

XRD. (2015). **OASIS: Extensible Resource Descriptor (XRD) V1.0**, retrieved from <http://docs.oasisopen.org/xri/xrd/v1.0/xrd-1.0.html>

XRDS. (2015). **OASIS: Extensible Resource Identifier (XRI) Resolution V2.0**, retrieved from <http://docs.oasisopen.org/xri/2.0/specs/xri-resolution-V2.0.html>.

XRI. (2015). **OASIS: Extensible Resource Identifier (XRI) Syntax V2.0**, retrieved from <http://docs.oasisopen.org/xri/xri-syntax/2.0/specs/cs01/xri-syntax-V2.0-cs.html>.

Yasir, S., Muhammad, I., Muhammad, A., Muhammad, B., Muhammad, H., Muhamamd, F., Amjad F., and Abad, S. (2012). **High Security and Privacy in Cloud Computing Paradigm through Single Sign On**. Life Science Journal, 9(4)

Zeilenga, K. (2006). **RFC 4524 – COSINE LDAP/X.500 Schema**. Internet Engineering Task Force (2006).