International Journal of Engineering & Technology, *7 (2) (2018) 732-741*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i2.10410
Review paper

Security strategies for cloud identity management - a study

Chunduru Anilkumar [1], Sumathy S [2] *

[1] Research scholar, SCOPE, Vellore Institute of Technology, Vellore, Tamilnadu-632014, INDIA.
[2] Associate Professor, SITE, Vellore Institute of Technology, Vellore, Tamilnadu-632014, INDIA.
**Corresponding author E-mail: ssumathy@vit.ac.in*

Abstract

Emphasis on security for providing Access Control in Cloud computing environment plays a significant role. Cloud computing provides number of benefits such as resource sharing, low speculation and large storage space. Huge amount of information stored in cloud can be accessed from anywhere, anytime on pay-per use basis. Resources in cloud should be accessed only by the authorized clients. Access Control in cloud computing has become a critical issue due to increasing number of users experiencing dynamic changes. Authentication, authorization and approval of the access ensuring liability of entities from login credentials including passwords and biometric scan is essential. Also, the federated authentication management is secured. Current approaches require large-scale distributed access control in cloud environment. Data security and access control are the drawbacks in existing access control schemes. Due to the drawbacks in existing access control schemes such as privacy of information when susceptible information is stored in intermediary service provider a federated identity access management is essential. Access control applications majorly concentrate on Healthcare, Government Organizations, Commercial, Critical Infrastructure and Financial Institutions. This review illustrates a detailed study of access control models in cloud computing and various cloud identity management schemes.

Keywords: *Cloud Security; Identity Access Management; Single Sign-on (SSO); Privacy; Open Id Connect; Federated Identity Management*

1. Introduction

Access Control is an authentication system that authorizes an authority or enables control access. While accessing the facility in general, various steps like authentication, authorization, identification and accountability are performed in access control system[1]. Clients are allowed to use the facility based on their identity. There are three characteristics to verify information with respect to access control devices such as PIN, PWD and Pass-Phrase, and the client has access through smart card along with finger print[2]. The technology is applied in biometric reader, card reader, door lock, door phone, locks etc. Security and trust aspects are significant snags of an organization to utilize distributed computing. Powerful identity and access management (IAM) is essential to reduce the security issues of distributed computing [3]. The emerging demand of external information handling and capacity rises various objections for sectors that need to prolong access control approaches apart from their organization's firewall into the cloud especially for outsourced information and maintenance [4]. Presently PC based software is used for log entries, where it maintains attendance with recorded in and out times. The main features of identity and access management system is Single Sign-On (SSO) [5]. Identities within the context are federated identities. Central Authentication Service (CAS) performs distributed identity and it also presents architecture for distributed identity services in cloud dependent technologies. In federated identity management design, such as OpenID Connect, it does not require registration in cloud for accessing [6]. However, incorporation between identity management and cloud computing is still a trail- particularly with respect to privacy and security issues [7]. Federated identity management systems utilize OpenID Connect and Shibboleth [8]. Privacy states to the capability of the people to protect data [9]. Everywhere in the world laws are proposed in order to take care of security in digital environment. Only on measuring privacy, the attributes and required data essentially utilized for access and identification have to be released [10].
Certainly, these designs cannot solve the problem, since one user shares his identity across multiple clouds (i.e. Single Sign-On). By using Single Sign-On and OAuth Protocol on one user, users can able to share their content to several clouds and also several users can share their content to single cloud [11]. These current advancements make the consolidation of IAM for distributed computing fascinating subject to research. The hazards and controls of IAM in distributed computing are analyzed in this paper. The detailed analysis of reports acknowledges the following four major trends in IdM.

a) Cloud-Dependent Identity Management
b) Powerful Client Management
c) Developing Bring Your Own Device (BYOD) mechanism
d) Application of attribute-based access control (ABAC)

This paper is structured as follows: first part presents the literature survey followed by a description of Access Management in Cloud computing in second and third section. Role of Identity Access Management in industry and IAM development in cloud environments are discussed in section four and five respectively. Preview of open issues are discussed in section six. Gap Analysis is explained in seventh section. Conclusion and Future work is briefed in section Eight.

2. Literature survey

Access control system provides an expert to control access in the system-based data framework or the resources in a physical facility [12]. By using cryptographic approaches, verifiable secure time-domain attribute- based access control (TAAC) scheme and session keys in the video contents are encrypted [13]. Attribute-based cryptosystem (ABC) lengthens identity-based cryptosystem (IBC) with adaptability and flexibility. Generally as an alternative explicit identity, various number of attributes are used to distinguish a user [14]. The complication of attributes benchmark in system and resolutions may happen during ABAC in right to use control for outsized scale systems like cloud [15]. Researchers working on privacy and security have explored on how to maintain the privilege of control, its revelation and location data [16]. The use of right to use control in cloud is to intercept the right to use on object in cloud by uncertified clients of cloud which tends to increase security in distributed environment [17]. Industrial efforts incorporate to provide cloud auditing in cloud environment. For example, Microsoft proposes SecGuru [18] to review Azure datacentre a group of policies utilizing the SMT solver Z3. IBM additionally gives the set of monitoring tool incorporated with QRader [19]. Amazon presents metric data and web API logs to their AWS clients by CloudTrail & AWS CloudWatch [20] that could be utilized for the reviewing purpose.

The MAC representation implements high security convenient in OS. Earlier, for secure data access they introduced access control mechanisms. Access control depends on security of the system and gives the access to the object [21]. Even though an administrator is present, it is very much constrained to define the policy [22]. With the extremity of more enlightened malware, such as Stuxnet, malware started to target program starting points that are left exposed [23]. At present many important organizations use identity management, such as IdM4Cloud, Novell Identity Manager, Microsoft Identity & Access, McAfee Cloud Identity Manager, etc [24].

The following are different access control mechanisms: Discretionary Access Control, Mandatory Access Control, Attribute Based Access Control, Role Based Access Control, and Identity Access Management.

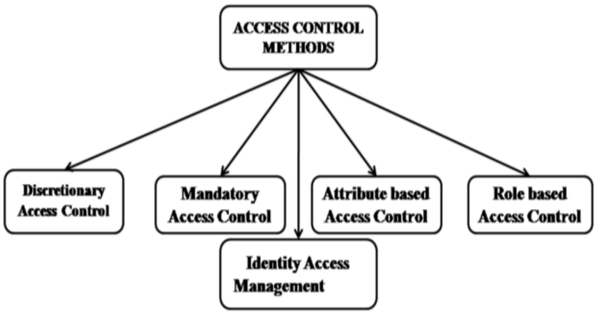
ACCESS CONTROL METHODS
Discretionary Access Control
Mandatory Access Control
Attribute based Access Control
Role based Access Control
Identity Access Management

Fig. 1: Classification of Access Control Methods.

2.1. Discretionary access control (DAC)

DAC mechanism fails to recognize the difference between computer program and human user. The subject decides object access constitutional rights. This is the model right to use control provided by file accessing and sharing [25]. It is generally at the caution of the owner of the object i.e., file or directory. DAC is adaptable in terms of policy identification. Access control generally resolves in typical multi-user platforms such as UNIX, Novell, etc [26]. Security concern is moving from industry solutions to cloud, due to data leakage issue in information sharing.

Table 1: Comparison of Discretionary Access Control

Author	Approach	Benefits	Gaps
Trent Jaeger et .al (1995)	Discretionary Access Control Model for Script-based Systems	Command script can be changed depending upon writer and the application on using access rights	To provide access rights Securely to the command script.
Ninghui Liet.al(2005)	safety is undecidable in Discretionary Access Control	Determines safety with running time O(n^3) in the Graham-Denning plan	Creating a set of labels using size of the linear state object.
Qihua Wang et .al(2011)	Data Leakage Mitigation for Discretionary Access Control in Collaboration Clouds	On reducing the errors in the choices of beneficiary for designing an attribute based recommender	Attribute-based Recipient recommender and abnormality detection.

2.2. Mandatory access control (MAC)

It protects a centralized administration of private security policy parameters. Its policy depends upon network configuration[27]. MAC models control access based on the awareness of subjects and objects. MAC arrangement is also known as multilevel security model and lattice-based access control. No method exists to verify the properties of MAC policy if they are exactly communicating a model and if the policy is contented in the execution.MAC arrangement can rectify the DAC problems with the DAC arrangement in more than one level environment i.e., army and government systems[28]. The main advantage of MAC is its directness; majorly it provides more security because only a system manager can access control.

Table 2: Comparison of Mandatory Access Control

Author	Approach	Benefits	Gaps
Vikhyath Rao et.al (2009)	Dynamic Mandatory Access Control for Multiple Stakeholders.	Benefits to understand security in SELinux deployment in a distributed environment	A local proxy server by using remote proxy server SELinux is required
M. Blanc et .al (2012)	Improving Mandatory Access Control for HPC clusters	Combining of new users and requests on using access control network file system on high bandwidth.	To solve the inconsistency between SELinux and Lustre to add the provision of contexts on NFS file system.
HayawardhVijayakumar et. al (2012)	Finding Attack Surfaces from Mandatory Access Control Policies	For requests based on MAC policy and a runtime method to precisely identify attack surface entry points in programs	To take privileges from web server through policies.

2.3. Attribute based access control (ABAC)

ABAC consists of policy agreement services that assesses digital approach against attributes. ABAC uses attributes as part of logical language, with its rules and requirements. Attributes are the group of labels or resources that can explain all the entities for approval principle [29]. Every attribute has a key value pair i.e. “Role=Supervisor”. Generally, attributes are isolated such as User, Subject, Object, and Context; Attribute (Meta-data) and so on. Basic components of ABAC are: Protocol Store, Protocol Editor, Protocol Information Point, Protocol Decision Service, and Protocol Enforcement Point. One of the standard application feature and policy based right to use control is Extensible Access. In ABAC [30], data access invitation is approved based on the client’s attributes, wherever files or data are allocated with expressive attributes. Figure 2 provides architecture with a request or response scheme.

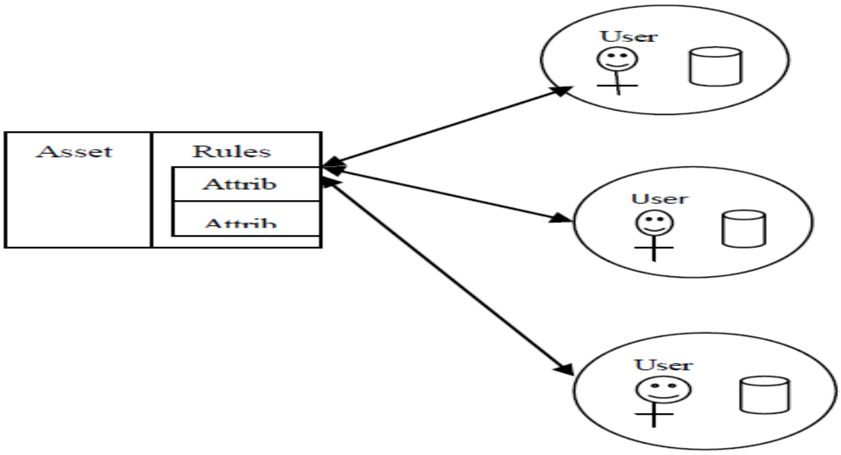

Fig. 2: ABAC Architecture.

Table 3: Comparison of Attribute Based Access Control

Author	Approach	Benefits	Gaps
Win-Bin Huang et.al (2015)	A Threshold-based Key Generation Approach for Cipher text-Policy Attribute-Based Encryption	Computation transparency is elevated compared to the key generation algorithms: ABE, KP-ABE, and CP-ABE.	Identity Access Management
Qi Li et.al (2016)	Secure, efficient and revocable multi authority access control system in cloud storage	Access Policy is flexible in Security provisioning	Attribute-level user revocation
Kan Yang et.al (2016)	Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing	A verifiable time domain ABE scheme in both cipher text and the keys can hold sufficient attributes and decrypt the data in particular time.	The attribute level users can access multiple time slots.
Balamurugan B et.al (2017)	Attribute Based Hierarchical Structure and Token Granting System using Cloud Computing Environment through secure access control	Limited access through the hierarchical structure, which is an arrangement of general attributes and users distinctive by Storage Correctness, and Fine-grained Access Provision (SCFAP).	Outsourced Data Decryption technique.
Junshe Wang et.al (2017)	Access Control Based Resource Allocation in Cloud Computing Environment	Cloud users get permissions dynamically on using Fuzzy Analytic Hierarchy Process	Resource Utilization using Access Control-based Resource Allocation (ACRA).
Antonious Gouglidis (2017)	Verification of Resilience Policies that Assist Attribute Based Access Control	The verification resilience is done using an automated model checking technique.	Combination of Security and Resilience in access control.
Sabitha S et.al (2017)	Access control-based privacy preserving secure data sharing with hidden access policies in cloud	Privacy conserved fine-grained access control-based information sharing in the public cloud	Hierarchical decentralized ABAC that incorporates secret policy and signature methods

2.4. Role based access control (RBAC)

It is a technique of control right to use network or computer facility based on the roles of independent clients within an activity. In this circumstance, right to use is the power of being user to conduct an explicit task, like analysis, modify, or create a file[31]. Roles are explained according to job skill, esteem and authority within the activity. Several managements depend on access control opinion on “the roles that independent users take on as part of management” [32]. RBAC model has reviewed three dimensions, because it has high probability of information leakage in Multitenancy environment. The three-dimensional role is explained as a vector power of authority, scope and permission time. It is compulsory for multi tenancy cloud platform to have characters of isolation and role hierarchy. RBAC perception bears three outstanding security frameworks. They are Least Privilege, Separation of Duties and Data abstraction.

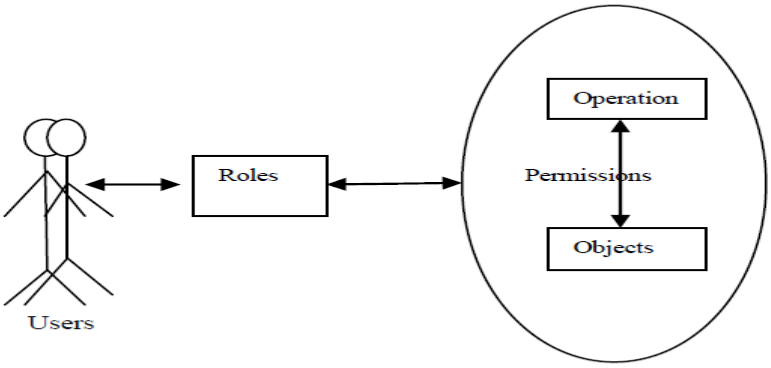

Fig. 3: Role Based Access Control Architecture.

Table 4: Comparison of Role Based Access Control

Author	Approach	Benefits	Gaps
Xingguang Zhou et.al (2016)	Role-Based Access Control on E-Health Records	Online / Offline approach of velocity in data handling to conduct EHR encapsulation and key generation.	Semantic privacy can be done using decisional bilinear assumptions.
Syed Zain R. Rizvi et.al (2016)	Interoperability of Relationship- and Role-Based Access Control	Constraints are verified by authorization time, and Satisfiability Modulo Theories (SMT) solving	Extend ReBAC to include a richer guard language for explaining critical requirements
Deepshikha Sharma et.al (2016)	Role based Access policy for enterprise data in cloud	ABE has built on RBAC framework for endeavor data.	For better key revocation technique, structure mechanism along with Identity-based and attribute based encryption mechanisms to resolve fine grained access control.
DivyaPritam et.al (2016)	Authentication and Encryption Techniques for Secure Data Storage in Cloud for Enforcing Role-Based Access Control	• RBAC policy to manage the custom of Data Owners information • Storing the information after encryption.	The spotlight is on data storage space and information security in the cloud environment, to build expectation assurance between client and cloud utility provider.
Alshreef Abed et.al (2017)	Naming Conventions scheme for role based access control in cloud based ERP Platforms.	The naming convention for search and user classification provides better results than Web Service Level Agreement (WSLA).	Simplify model to carry access to several facilities along with a central replicated database.

2.5. Identity access management (IAM)

Identity management (IdM) is the procedure of managing and creating and infrastructure that gives support to these processes. Exchanging data and resources are dynamically cooperated by IdM systems in cloud environments [33]. The suggestions given by the National Institute of Standards and Technology (NIST) IAM are known as the critical research area [34]. For any online service in private, public and hybrid cloud they facilitate the resources of sharing among partners is Federated Identity Management Systems (FIdM) [35].

Table 5: Comparison of Identity Access Management

Author	Approach	Benefits	Gaps
Elisa Bertino et .al(2009)	Privacy-preserving Digital Identity Management for Cloud Computing	On addressing heterogeneous naming, efficient cryptographic protocols and techniques are used	To maintain control between multiple transactions same user and different CSP can carry that out.
Antonio Celesti et .al(2010)	Inter Cloud Identity Management Infrastructure (ICIMI)	Reference architecture addresses the Identity Management and shows how federated environment is managed.	The performances of ICIMI, evaluating the IdP enrollments and authentications are needed on simulated environments.
Safiriyu Eludiora et.al(2011)	A User Identity Management Protocol for Cloud Computing Paradigm	The user identity management protocol is used to secure data at all levels.	Billing services are design for cloud computing
Umme Habiba et .al(2014)	Cloud identity management in security	On using distributed system degree of connectivity and usage are changing.	Cloud based identity management systems (IDMS) can be designed and develoed for access control.
Jorge Werner et .al (2017)	Cloud identity management in privacy strategies.	To reduce breaching in cloud environment for identity management.	Lack of user preference guarantees on the Service Provider side.
Davy Preuveneer et.al(2017)	Identity management for cyber-physical production workflows and individualized manufacturing	Supports Privilege defense-in-depth security approach	Dataflow oriented processes to assure the authenticity and trustworthy access of users.
Nasser Abdulla et.al(2017)	Identify Cloud Security Weakness related to Authentication and Identity Management (IAM) using Open stack keystone Model	Use an unrestricted network to switch the SAML (Security Assertion Markup Language) ticket between the user in the internet application services for Single-Sign-On.	The integrity and authentication of SAML token and exchange of token through secure communication channel (SSL).

3. Access management in cloud computing

For accessing Public Cloud Services, internet connection is required, instead of local network connection [36]. Local network is very easy to manage than internet and moreover, local network can be managed by the organization itself. Internet can be accessed by anyone with compatible devices, because it is a public network [37].

The following are the risks applicable to access management in a multitenant virtualized environment.

a) Rules and Regulation risks
b) Technology Risks
c) Operational Risks
d) Data Risks.

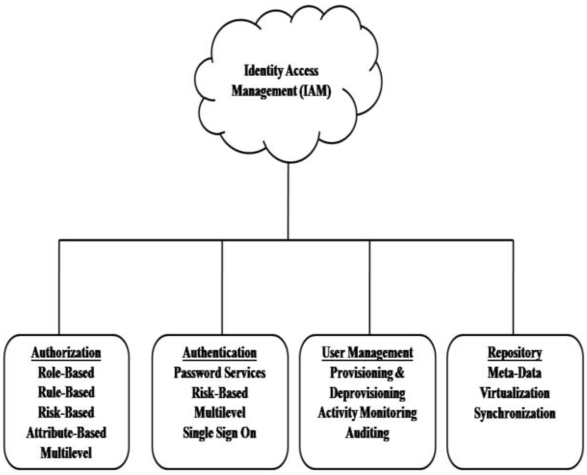

Fig. 4: Identity and Access Management (IAM) Components.

Identity management (IdM) is the procedure of managing, creating, using identities and extending support for these processes. In IdM, every person is analyzed by a credential, which produces a set of attributes, issued by the stable source [38] [39]. Each person has a credential suppressed by his/her birth date and name. Every application has an identifier, URL, and public key in its credentials[40]. In IAM systems, utility and identity providers are IdM components dealing with authorization and authentication in the environment. [4]

3.1. Authentication

This is the basic step before allowing anyone to perform an operation in a system. Authentication is performed in IdP, which reserves the attributes of users[41]. After completion of authentication, IdP sends a request or credential to the service provider.

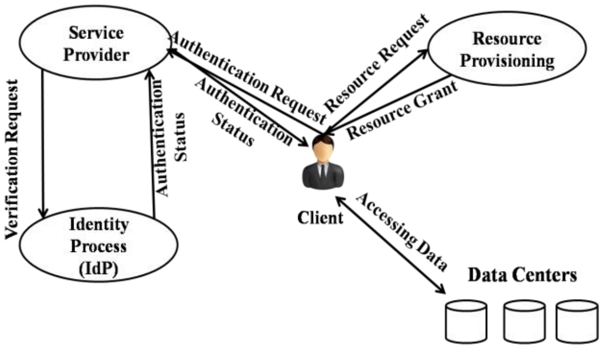

Fig. 5: Identity Access Management Architecture.

Client sends authentication request to the service provider (SP). SP sends verification request to Identity Process (IdP) and on receiving acknowledgement of the authentication status sends acknowledgement to the client in turn (Figure 5). Further, client sends resource request to resource provisioning module, and receives resource grant. Subsequently, data from data centers are accessed by the clients[42].

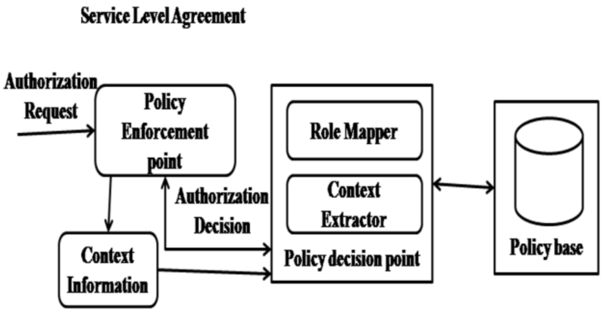

Fig. 6: Identity Process Architecture.

An IdP plays a vital role at each level to apply the right to use control policy. As mentioned in Figure 6, the main mechanism of IdP includes:

- A policy decision point
- PEP (policy enforcement point) and
- A policy supports

PEP includes the requesting subject, requesting reserve, and the permission requested for that reserve (Figure 6).

3.2. Authorization

The type of access is based on the identity of the person, or part of the system that needs to be accessed. The authorization process is carried out in SP, using requests received from IdP [43]. In addition to offering highest security in identity handling, one of the advantages of using identity access management system is the capability to use Single Sign-On (SSO) [44]. With SSO, from single evidence in the home domain or IdP, the user is able to use other services in the circle of trust or same domain [45]. Action of closing all sessions of access, with single sign out process is named as single sign-off.

Federated Identity Management System (FIdM) is important for any online service in a private, public, and hybrid cooperation system [46] because it promotes the sharing of resources to partners.

The following are the functions of IAM:

- Identity Management in the cloud
- The Single Sign-On (SSO) and federated identity implementation possibility assurance
- Authorization Management
- Compliance Management

Validation of both services and clients is a major problem for the assurance and security of the distributed computing. Identity based ranking model for distributed computing and its interrelated signature and encryption pattern, conferred a new identity-based validation protocol for distributed computing and utility.

4. Role of identity access management in industry

The following are the Real Time Cloud providers in Industry.

- Amazon EC2
- IBM Blue Mix
- Microsoft Azure
- Google Cloud
- Dream Host

4.1. Amazon EC2

IAM is a web utility which authorizes AWS (Amazon Web Services). Clients can have direct control over user permissions and users in AWS[47]. On Using IAM, security credentials can be managed. This service is majorly concentrated on organizations with many users that use AWS products such as Amazon Sample DB, Amazon Managing Console, and AWS Command Procession Tools, AWS SDKs, and IAM HTTPS API.

In Amazon EC2, the following are the features of IAM.

- Shared admittance to AWS report.
- Granular Permissions
- Integrity Federation
- Identity data for oath
- Protected right of entry to AWS assets for applications that scamper on Amazon EC2.

4.2. IBM blue mix

With identity and access management, we are expert to identify and authorize a user, arrange user specific access to cloud resources, and applications [48]. In cloud Environment different types of roles are going to manage.

- Administrative users
- Developer Users
- Application Users

When we are going to implement identity and access management for an application, the following are the authentication models are used [49].Unprotected Websites, Website for internal employees and users, Website with an existing customers audience, Website with an audience of suppliers, Website with a new customer audience.

4.3. Microsoft azure

Many developers are not self-experts and generally they don't want to spend more time developing authorization and authentication mechanisms for their services[50]. Microsoft Azure provides easy way to client authentication by using access control services in order to use web applications. An Identity Provider (IP) is control that validates identities and security tokens. The original work behind providing the tokens is executed through a unique service called Security Token Service (STS). Examples of IPs include, Face book, Windows Live ID. Access Control Service can belief more IPs at a time that means application beliefs ACS, then instantly offers application to all users for all IPs.

4.4. Google cloud

Google Cloud provides Identity and Access Management (IAM) that gives direct access in to the specific Google Cloud and verifies forbidden entry to other resources. IAM policies grant roles to a user, and they are giving certain permissions. Every Google Cloud DNS API method required necessary IAM permissions[51]. Permissions are assigned by granting roles to a user, or service account. Permissions allow users to perform specific actions on resources. IAM permissions allow users to run XML and JSON methods on objects.

4.5. Dream host

Dream Host offers different set of identities required by companies for each service provider, the nature of cloud computing raises to establish relationship[52]as a federation in cloud providers. The distribution of private data should be managed, rather than user agreement.

5. IAM development in cloud environment

The following are the IAM development in cloud.

- Validation Managing
- Client Managing
- Authorization Managing
- Access Managing
- Information Managing and Provisioning
- Monitoring and examine
- Risk Per dimensions

5.1. Validation managing

Validation Managing is one of the major sections of IAM with the intention of regularly not to take care of industries that use cloud utility. In every CSP having their possess verification method for clients to access the cloud utility. For Example, Google Apps, Sales force and Microsoft Office 365 are using their own authentication mechanism [53].

Table 6: Rank of Control in Validation Managing

IAM Planning's	Rank Of Control
Traditional Model	Low
Trust Correlation Model	High
Identity Utility Provider Model	Medium
All in the Distributed Model	Low

It can modify the requirements and mechanisms, if CSP has authority of authentication. It is a risk position in the industry if the cloud service is not in control of changes. The following are the risks relevant to verification managing for various models in distributed environment.

Table 7: Validation Managing Risks

Risks	Description
Information Risks	Failure due to various security necessities for verification, Data theft
Operational Risks	Unable to manage changes in authentication mechanisms.
Technology Risks	Incompatible SSO. Incompatible authentication Mechanisms.
Law and Ruling Risks	Refusal with security policy.

5.2. Client managing

The following are the changes made after analysis of information managing process in cloud environment. Clients know how to change, reveal in the form of Cloud Data Service (CDS) of CSP. In conventional replica the industries can change and remove clients with in CDS of the CSP. In all in the distributed model, clients are stored in the CDS of the CSP that grants the IAM Services. The major difference of information managing while using the cloud services is in the failure of control in excess of CDS.

Table 8: Rank of Control in Information Managing

IAM Planning's	Rank of Control
Traditional Model	Low
Trust Correlation Model	High
Identity Utility Provider Model	High
All in the Distributed Model	Low

By unauthorized users, the integration of client's data is insecure, not confidential and personal details can be viewed or even changed by unauthorized clients. The service will be very difficult to deploy. The CSP does not support the mechanisms to accumulate and inform client's information to the industry purpose.

Table 9: Client Managing Risks

Risks	Description
Information Risks	Loss clients data due to incompatible data security requirements, Data theft
Operational Risks	Not capable to justify winning inform of CDS No manage to make changes to client managing by CSP.
Technology Risks	No compatible technology is using to update and store the client's data.
Law and Ruling Risks	Based on personal information local laws and regulations with no compliance.

5.3. Authorization managing

The major difference for authorization models, both industries and CSP using the Cloud services. It is difficult to integrate authorizations of clients, industries are going to implement (RBAC) role based access control model to conduct authorizations and CSP does not hold [54].

Table 10: Rank of Control in Authorization Managing

IAM Planning's	Rank of Control
Traditional Model	High
Trust Correlation Model	High
Identity Utility Provider Model	High
All in the Distributed Model	High

If data is modified or removed, access of the security requirements cannot be met. In industries, authorizations for errors can check manually at the CSP. In Industries cloud services are unable to check, if authorizations of clients are followed by the CSP.

Table 11: Authorization Managing Risks

Risks	Description
Information Risks	If authorizations cannot be integrated unauthorized data can be modified.
Operational Risks	Unable to authenticate authorizations for errors Unable to authenticate successful performances of authorizations.
Technology Risks	---------
Law and Ruling Risks	If the authorizations cannot be integrate then non-compliance with laws and regulations.

5.4. Access managing

The main difference for access management in industries cloud services are not under the control of compulsion of their security policies for the services of CSP. Access to their services is under the control of CSP. For accessing public cloud services internet connection is required instead of using local network connection. Controlling the local network connection is easier than controlling by the internet, because local network is maintained by industry itself.

Table 12: Rank of Control in Access Managing

IAM Planning's	Rank of Control
Traditional Model	Low
Trust Correlation Model	Low
Identity Utility Provider Model	Low
All in the Distributed Model	Low

If the data is not appropriately protected, in industries any one can access the data using internet in cloud services. Industry can be incompliance because data can be secured by laws or regulations. [55]. If connections of CSP fail, the cloud services cannot be accessed by the industry

Table 13: Access Managing Risks

Risks	Description
Information Risks	Industry's data are in general because of virtual and physical.
Operational Risks	Unable to check who has or had access to information.
Technology Risks	It stops the accessing of cloud services because, failure of internet connection.
Law and Ruling Risks	Data secured by laws or regulations because of virtual and physical.

5.5. Information managing and provisioning

There are some differences in provisioning and information managing in cloud environment. Client's accounts have been provisioning and de-provisioning at CDS of the CSP in all in the cloud and traditional model. In identity service provider model and trust relationship model the clients are provision in local CDS of the industry by means of cloud utility, Provisioning as well as de-provisioning is forbidden by it.

Table 14: Rank of Control in Information Managing and Provisioning

IAM Planning's	Rank Of Control
Traditional Model	Low
Trust Correlation Model	Medium
Identity Utility Provider Model	Medium
All in the Distributed Model	Low

According to the security standards and regulations requirements for encryption and removal cannot be implemented[56]. If the technology is not compatible with the industry, cloud services may not be providing client accounts to the CSP. Authorized users cannot be access the resources.

Table 15: Data Management and Provisioning Risks

Risks	Description
Data Risks	Data loss due to wrong de provisioning Data loss due to various data security requirements.
Operational Risks	Unable to prove standard of provisioning and data management. Unable to control modifications in provisioning and data management.
Technology Risks	Due to wrong provisioning it can't access authorized resources.
Law and Regulation Risks	Unofficial access to data saved by laws and regulations

5.6. Monitoring and examine

In the traditional IT environment, the industries can audit and monitor its own network and systems. While using cloud services the industries do not have control over the IAM. Industries cannot audit the CSP, which stores the data and runs a part of IAM processes.

Table 16: Rank of Control in Monitoring and Examine

IAM Planning's	Rank Of Control
Traditional Model	Low
Trust Correlation Model	Low
Identity Utility Provider Model	Low
All in the Distributed Model	Low

They are not capable to audit and monitor cloud utility which makes it complex to identify unauthorized access to information [55].They use cloud services and not the control of frequency, auditing, logging, etc.

Table 17: Monitoring and Examine Risks

Risks	Description
Information Risks	Data loss due to undiscovered illegal access to data or Data Theft.
Operational Risks	Cannot control the frequency of monitoring, logging, quality and auditing.
Technology Risks	Technical problem cannot be solved due to monitor cloud services.
Law and Ruling Risks	If the CSP cannot be inspection because of noncompliance and regulations.

5.7. Risks per dimension

To design the risk investigation for every part of IAM, risk dimensions are used. To get an overview of all relevant risks for IAM in a distributed environment, risk is combined in every risk dimension. The following are risks per dimensions in cloud surroundings.

a) Law and Ruling Risks.
b) Information Risks.
c) Technology Risks.
d) Operational Risks.

5.7.1. Law and ruling risks

Risk of inflexibility to laws and regulations due to law and regulation risk arises. In cloud computing environment these risks are specified below for the relevant laws and regulation risks.

Table 18: Law and Ruling Risks

Law and Ruling Risks	Description
	Failure with relevant laws on location of information Failure with relevant inspection on regulations Failure with relevant laws on personal data Failure with relevant convention on refuge needs

5.7.2. Information risks

Combining the outcome of research to facts risk, outcome is in the risk of data theft or loss. These risks are described in depth below for the different factors.

Table 19: Information Risks

Information Risks	Description
	Data depletion or stealing due to wrong de-provisioning. Data depletion or stealing due to various information protection needs Data depletion or stealing due to anxious authentication Data depletion or stealing due to unsuitable authorization control Data depletion or stealing due to lack of inspection capabilities and control Data depletion or stealing due to natural access of hardware that contains information.

5.7.3. Technology risks

The subsequent technology risks are familiar after combining the analysis to various parts of distributed environment in IAM.

Table 20: Technology Risks

Technology Risks	Description
	Not Compatible with SSO Not Compatible with authentication mechanism Not Compatible with technology to update or store the client's data. Stop accessing the cloud services because of failure of internet connection. Due to wrong provisioning not able to access the cloud services. Due to failure of monitor the services not able to solve technical issues.

5.7.4. Operational risks

Combining the results of operational risks of IAM in cloud environment results in difficulty to manage in industries, and verify IAM. The risks are detailed below for various factor those principles apply.

Table 21: Operational Risks

Operational Risks	Description
	Not able to use principle modifications to processes. Not able to authenticate strong updates of clients' accounts Not able to authenticate authorization for failures Not able to authenticate successful hit of authorizations Not able to authenticate who had or has accessing the information. Not able to authenticate provisioning and character of data management. Not able to authority the logging, frequency of monitoring and inspection.

6. Open issues

DAC:

- It can be easily compromised by third parties and it is possible to take the copy of unique message without owner's consent.
- There is no proper assurance regarding the flow of information.
- Trojan horse Threads.

MAC:

- MAC desires to dispatch the related utilities and operating system in light of the access control frame work.
- MAC models place limits on users access and according to protect policies does not tolerate self-motivated alteration.
- MAC requires determined setup to implement efficiently. After implementing it desires an elevated organization management to continuously update object and account labels to collect new data.

RBAC:

- The roles in a special perspective are complicated and it may result in huge role description. Occasionally it produces extra roles than users.
- RBAC allocates the roles statically to its user, which is not chosen in dynamic environment. It is hard to put into practice when the environment is energetic and distributed.
- It is more complicated to alter the access rights of the user without varying the role of that user.
- RBAC does not recommend for dynamic attributes such as time of the day on which the user agreement is determined.
- To implement the RBAC model roles it should be assigned in advance and it is not likely to modify access rights without changing the roles.
- Permissions connected with each role can be deleted or distorted based on the advantage of role change.

ABAC:

- In Multi-tenant multi-cloud federation, extension of current approaches to heterogeneous cloud platforms in addition to policy integration issues in heterogeneous multi-cloud IaaS needs focus.
- Multi-tenant ABAC can be explored to cover contextual and environmental attributes. Administrative model is another motivating extension of MT-ABAC.
- Extending Multi-tenant Authorization as a Service Open Stack API to support attribute-based MTAC models.
- Tenant cannot arrange their own policy. Users cloud role policy is as an alternative.
- Not able to arrange tenant administrator.
- ABAC does not offer the user role assignment concept.

IAM:

- Multilevel security to raise fine-grained on demand access control model.
- Lack of Personal Identifiable Information (PII).
- Lack of frameworks to support clients in data distribution during information exchange.
- Lack in Service Provider's (SP) in assuring user's performance.

7. Gap analysis

It is clear from the literature that the techniques incorporating DAC and MAC are not suitable for current security advancement techniques. ABAC and RBAC can cope up with current requirements which are not widely used presently. IAM is the latest and popular area of research that has wide scope and can be studied for further enhancement. As many applications are susceptible from attacks in many ways, if and only if the advancements in security techniques evolve, security policies can withstand.

8. Conclusion & future work

A survey on isolation feature in the cloud, describing identity management in multitenant virtualization environment is presented. Initially, Identity Management Model with isolation is proposed in cloud environment that exhibits the feature solutions offering minimization, transparency and controllability to reduce the risks of privacy. A performance measure using OpenID Connect protocol, working with JavaScript Object Notation (JSON) instead of Security Assertion Markup Language (SAML), is easier to use in cloud environments. A work flow relation between the Identity Management (IdM) and System (SP and IdP) is analyzed and presented. Further, privacy interaction between IdP and SP will be focused in order to study the privacy aspects for the interactions.

References

[1] Y. Yang, X. Chen, G. Wang, and L. Cao, "An Identity and Access Management Architecture in Cloud," 2014 *Seventh Int. Symp. Comput. Intell. Des,* vol. 2, pp. 200–203, 2014. https://doi.org/10.1109/ISCID.2014.221.

[2] A. Bhargav-Spantzel and S. W. Deutsch, "Platform capability based identity management for scalable and secure cloud service access," *2012 IEEE Globecom Work. GC Wkshps 2012*, pp. 763–768, 2012.

[3] Novell, "Identity and Access Management in the Cloud," *Cloud Secur. Alliance Res. Pap., pp*. 3–19, 2010.

[4] N. K. Shukla, "IDENTITY & ACCESS MANAGEMENT."

[5] A. Pereira, J. Sobral, and C. Westphall, "Towards scalability for federated identity systems for cloud-Based environments," *2014 6th Int. Conf. New Technol. Mobil. Secur. - Proc. NTMS 2014 Conf. Work.*, 2014.

[6] V. Nirmala, "Hierarchical Identity Role based proxy re-encryption scheme for cloud computing," pp. 19–22, 2013. https://doi.org/10.1109/ICACCS.2013.6938719.

[7] Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., & Waidner, M. (2004). Privacy-enhancing identity management. *Information security technical report,* 9(1), 35-44. https://doi.org/10.1016/S1363-4127(04)00014-7.

[8] Weingärtner, R., & Westphall, C. M. (2014). Enhancing privacy on identity providers. *SECURWARE 2014, 93.*

[9] Landwehr, C., Boneh, D., Mitchell, J. C., Bellovin, S. M., Landau, S., & Lesk, M. E. (2012). Privacy and cybersecurity: The next 100 years. *Proceedings of the IEEE, 100* (Special Centennial Issue), 1659-1673. https://doi.org/10.1109/JPROC.2012.2189794.

[10] Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud-computing environments: Challenges, taxonomy, and survey. *ACM Computing Surveys (CSUR), 47* (1), 7. https://doi.org/10.1145/2593512.

[11] M. Kunz, M. Hummer, L. Fuchs, M. Netter, and G. Pernul, "Analyzing recent trends in enterprise identity management," *Proc. - Int. Work. Database Expert Syst. Appl. DEXA,* pp. 273–277, 2014. https://doi.org/10.1109/DEXA.2014.62.

[12] W. Bin Huang, W. T. Su, and C. S. Liang, "A threshold-based key generation approach for ciphertext-policy attribute-based encryption," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, vol. 2015–Augus, pp. 908–913, 2015. https://doi.org/10.1109/ICUFN.2015.7182677.

[13] K. Yang, Z. Liu, X. Jia, and X. S. Shen, "Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach," *IEEE Trans. Multimed*., vol. 18, no. 5, pp. 940–950, 2016. https://doi.org/10.1109/TMM.2016.2535728.

[14] H. Zheng, J. Qin, J. Hu, and Q. Wu, "Threshold Attribute-Based Signcryption in Standard Model," *Proc. - 2nd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2015 - IEEE Int. Symp. Smart Cloud, IEEE SSC 2015, pp*. 187–193, 2016.

[15] C. Ngo, Y. Demchenko, and C. De Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *J. Inf. Secur. Appl.*, vol. 27–28, pp. 65–84, 2016.

[16] I. Ray and M. Kumar, "Towards a location-based mandatory access control model," *Comput. Secur,* vol. 25, no. 1, pp. 36–44, 2006. https://doi.org/10.1016/j.cose.2005.06.007.

[17] T. Jung, X. Y. Li, Z. Wan, and M. Wan, "Rebuttal to "comments on 'control cloud data access privilege and anonymity with fully anonymous attribute-based encryption"'," *IEEE Trans. Inf. Forensics Secur,* vol. 11, no. 4, p. 868, 2016. https://doi.org/10.1109/TIFS.2015.2509946.

[18] Bjørner, N., & Jayaraman, K. (2015, February). Checking cloud contracts in microsoft azure. *In International Conference on Distributed Computing and Internet Technology* (pp. 21-32). Springer, Cham. https://doi.org/10.1007/978-3-319-14977-6_2.

[19] IBM Corporation, "Safeguarding the cloud with IBM security solutions," http://www.ibm.com, Tech. Rep., 2013.

[20] Amazon Web Services, "Security at scale: Logging in AWS,"http://aws.amazon.com, Tech. Rep., and November 2013.

[21] A. Ben Fadhel, D. Bianculli, and L. Briand, "GemRBAC-DSL : a High-level Specification Language for Role-based Access Control Policies," *Proc. 21st ACM Symp. Access Control Model. Technol. - SACMAT '16*, pp. 179–190, 2016. https://doi.org/10.1145/2914642.2914656.

[22] M. Blanc and J. F. Lalande, "Improving mandatory access control for hpc clusters," *Futur. Gener. Comput. Syst*., vol. 29, no. 3, pp. 876–885, 2013. https://doi.org/10.1016/j.future.2012.03.020.

[23] H. Vijayakumar, G. Jakka, S. Rueda, J. Schiffman, and T. Jaeger, "Integrity walls: Finding attack surfaces from mandatory access control policies," *ASIACCS 2012 - 7th ACM Symp. Information, Comput. Commun. Secur,* pp. 75–76, 2012. https://doi.org/10.1145/2414456.2414500.

[24] Alguliev, R. M., & Abdullayeva, F. C. (2013, August). Identity management-based security architecture of cloud computing on multi-agent systems. *In Innovative Computing Technology (INTECH), 2013 Third International Conference on* (pp. 123-126). IEEE.

[25] Q. Wang and H. Jin, "Data leakage mitigation for discretionary access control in collaboration clouds," *Proc. 16th ACM Symp. Access Control Model. Technol. - SACMAT '11*, p. 103, 2011. https://doi.org/10.1145/1998441.1998457.

[26] N. Li and M. V. Tripunitara, "On safety in discretionary access control," Proc. - *IEEE Symp. Secur. Priv*., pp. 96–109, 2005.

[27] V. C. HU, D. R. KUHN, T. XIE, and J. HWANG, "Model Checking for Verification of Mandatory Access Control Models and Properties," *Int. J. Softw. Eng. Knowl. Eng*., vol. 21, no. 1, pp. 103–127, 2011. https://doi.org/10.1142/S021819401100513X.

[28] X. Zhang, M. J. Covington, S. Chen, and R. Sandhu, "SecureBus: towards application-transparent trusted computing with mandatory access control," *ACM Symp. Information, Comput. Commun. Secur*, pp. 117–126, 2007.

[29] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "k -times Attribute-Based Anonymous Access Control for Cloud Computing," vol. 9340, no. c, pp. 1–13, 2014.

[30] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable and fine-grained data access control in cloud computing. *In Infocom, 2010 proceedings IEEE* (pp. 1-9). Ieee.

[31] A. Workflows et al., "Security Constraints in Temporal Role-Based," *Codaspy*, pp. 207–218, 2016.

[32] J. Li, Z. Liao, C. Zhang, and Y. Shi, "A 4D-Role Based Access Control Model for Multitenancy Cloud Platform," vol. 2016, 2016.

[33] J. T. Goulding, "identity and access management for the cloud : CA Technologies strategy and vision," no. April, p. 18, 2011.

[34] Jansen, W., & Grance, T. (2012). Guidelines on security and privacy in public cloud computing.

[35] E. Ghazizadeh, M. Zamani, J. L. Ab Manan, and A. Pashang, "A survey on security issues of federated identity in the cloud computing," *CloudCom 2012 - Proc. 2012 4th IEEE Int. Conf. Cloud Comput. Technol. Sci.*, pp. 562–565, 2012. https://doi.org/10.1109/CloudCom.2012.6427513.

[36] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "PRIAM: Privacy preserving identity and access management scheme in cloud," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 1, pp. 282–304, 2014. https://doi.org/10.3837/tiis.2014.01.017.

[37] J. Werner, C. M. Westphall, and C. B. Westphall, "Cloud identity management: A survey on privacy strategies," *Comput. Networks*, vol. 122, pp. 29–42, 2017. https://doi.org/10.1016/j.comnet.2017.04.030.

[38] Authentication, O. (2013). 2.0, OpenID Foundation, 2007.

[39] Shibboleth Consortium. Shibboleth Home Page.

[40] M. Hansen et al., "Privacy and identity management," *Secur. Privacy, IEEE,* vol. 6, no. 2, pp. 38–45, 2008. https://doi.org/10.1109/MSP.2008.41.

[41] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," *Cloud Comput*., 2009.

[42] M. Stihler, A. O. Santin, A. L. Marcon Jr., and J. D. S. Fraga, "Integral Federated Identity Management for Cloud Computing," *2012 5th Int. Conf. New Technol. Mobil. Secur*, pp. 1–5, 2012.

[43] M. V. Thomas, A. Dhole, and K. Chandrasekaran, "Single Sign-On in Cloud Federation using CloudSim," *Int. J. Comput. Netw. Inf. Secur*, vol. 7, no. 6, pp. 50–58, 2015.

[44] R. Baldoni, "Federated Identity Management systems in e-government: the case of Italy," *Electron. Gov. an Int.* J., 2012.

[45] H. Xiong, K.-K. R. Choo, and A. V. Vasilakos, "Revocable Identity-Based Access Control for Big Data with Verifiable Outsourced Computing," *IEEE Trans. Big Data*, vol. 6, no. 1, pp. 1–1, 2017. https://doi.org/10.1109/TBDATA.2017.2697448.

[46] K. E. U. Ahmed, V. Alexandrov, Z. Mahmood, and R. Hill, "Cloud Computing for Enterprise Architectures," *Media,* pp. 115–133, 2011. https://doi.org/10.1007/978-1-4471-2236-4_6.

[47] A. Lonea, H. Tianfield, and D. Popescu, "Identity management for cloud computing," *New concepts Appl. soft*, 2013.

[48] A. Gheith, R. Rajamony, and P. Bohrer, "IBM bluemix mobile cloud services," *IBM J.*, 2016.

[49] H. Lee, I. Jeun, and H. Jung, “Criteria for evaluating the privacy protection level of identity management services,” *Emerg. Secur. Information, 2009*.

[50] C. Kaufman and R. Venkatapathy, “Windows AzureTM Security Overview,” *Publ. Aug* 2010.

[51] N. Saravanan and A. Mahendiran, “An implementation of RSA algorithm in google cloud using cloud SQL,” *Res. J*, 2012.

[52] R. Pacevič and A. Kačeniauskas, “The development of VisLT visualization service in Openstack cloud infrastructure,” *Adv. Eng. Softw*, 2017. “G Suite.”

[53] H. Chang and E. Choi, “User authentication in cloud computing,” *Int. Conf. Ubiquitous Comput*, 2011.

[54] W. Jansen and T. Grance, “Sp 800-144. Guidelines on security and privacy in public cloud computing,” 2011.

[55] S. Carlin and K. Curran, “Cloud computing security,” 2011.