International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
International Conference on Communication Computing & Virtualization 2016

Transparent Identity and Access Management as Managed Security Service from Clouds

Deepak H. Sharma
Department of Computer Engineering,
K. J. Somaiya College of Engineering

C A. Dhote, PhD
Department of Computer Science & Engineering,
P. R. M. I. T & R,
Amravati

Manish M. Potey
Department of Computer Engineering,
K. J. Somaiya College of Engineering

ABSTRACT
In managed security model the focus is on security provided as cloud service; i.e. security delivered through the cloud instead of on-premise security solutions. Identity and Access Management (IAM) focuses on authentication, authorization, administration of Identities and audit. Its primary concern is verification of identity of entity and granting correct level of access for resources which are protected in the cloud environment. The IAM implemented as managed cloud service can benefit the user with all the advantages offered by Security-as-a-service model (SECaaS). This paper discusses implementation of a proof-of-concept (POC) of transparent managed IAM service. This prototype has been also evaluated. The relevant technologies are discussed for providing secure access to cloud users.

General Terms
Cloud Computing, Authentication, Authorization, Audit, Security Issues, managed security service.

Keywords
Managed Security Service, Security-as-a-service.

1. INTRODUCTION
Cloud Computing is a nascent and rapidly evolving model, with new aspects and capabilities being added regularly by researchers around the world. Cloud computing has its roots in large-scale distributed computing technology. It is in fact an extension of grid computing, distributed computing, and parallel computing [1]. Nicholas Carr equates the rise of cloud computing in the information age to electrification in the industrial age. Carr argues that in the emerging future organizations will simply plug in to cloud (computing grid) for the computing resources they need [2].

Managed Securitydelivered from cloud focuses on security delivered as one of the cloud services; i.e. security provided through the cloud instead of on-premise security solutions. The managed security model can enhance the functionality of existing on-premise implementations by working with them as part of hybrid solution as well. Identity and Access Management (IAM) consists of processes which are used to manage access to resources. This is done by verifying the identity of an entity, after verification of identity the access is granted at the appropriate level based on the policy of protected resource [3].

This paper proposesa transparent model of Identity and Access Management implemented as managed security service. In particular this managed IAM is an on-demand portable, transparent and available pay-per-use cost model. The paper addresses various issues regarding security delivered as cloud service. This paper addresses the following issues in separate sections. Section 2 discusses the related work. Section 3 discusses architecture and scope of proof-of-concept (POC) of managed Identity and Access Management, in Section 4 the POC is evaluated and Section 5 concludes the paper and discusses future work.

2. RELATED WORK
In Cloud Security Alliance (CSA) SECaaS defined category of service [4], the core functionalities of Identity and Access Management are defined as account provisioning/deprovisioning, authentication, authorization, policy management, role based access and federated single sign on.

In CSA SECaaS Implementation guidance [5], the IAM components include:

- Centralized Directory Services,
- Access Management Services,
- Identity Management Services,
- Identity Federation Services,
- Role-Based Access Control Services,
- User Access Certification Services,
- Privileged User and Access Management,
- Separation of Duties Services, and
- Identity and Access Reporting Services.

In [6] the authors have spelled out specific requirements of IAM, viz. User management, Authentication, Authorization, Monitoring and Auditing. The authors have also proposed Identity management as a service (IDaaS). Here the authentication is delegated to identity management service. The advantages discussed are reduced complexity of different Cloud service providers supporting different federation standards, minimal architectural changes from user's point of view to support this model.

In [7] the authors have proposed user-centric trust Identity service with an aim to create trust among Cloud Service Providers (CSP). Their model has Authentication, Authorization, and Provisioning and Audit modules along with the Trust agent. The federated environment will allow users to login to various Cloud Service Providers depending on the application access. When the user moves to different CSP the user credentials follow in the federated environment.

The Trust Agent in the Identity Management sends the Trust Token along with the user attribute which creates a trust between CSPs.

In [8] the authors have propose an Identity and Access Management architecture in cloud to achieve security requirement like Strong Authentication, Data Loss Prevention, Security as a Service. The various systems components for addressing the above security requirements are Cloud Resource provider, Identity Management, Policy Management, Resource Engine and Access Decision-making. The various advantages of their approach were Comprehensive identity management, standardized architecture, and scalable design.

3. POC IMPLEMENTATION OF TRANSPARENT MANAGED IAM

The focus here is on Identity and Access Management to be provided as managed transparent cloud service; i.e. security delivered through the cloud. Identity Management consists of management, creation and deletion of digital identities. Access Management is more granular, it consists of authorization of access of entity to protected resources. The requirements of secure Identity and Access Management, and the tools in use to provide IAM security in the cloud are as below:

- Authentication: Authentication is the process in which identity of an entity is verified when it is trying to access a protected resource. Authentication process must be secure and manageable. For certain secure cases where higher level of security is needed, multiple factor authentications are generally required.
- Identity Federation services: Federated identity services allow management of both the identity and access of its users to resources. This is usually done for partner organizations providing services authorized for the specific users.
- Authorization Management: Authorization in the cloud ensures that clients have appropriate rights to access protected resources in the cloud. It also helps secure various enterprise managed resources. It approves or disapproves the User access needs at run time with respect to the authorization policies of an organization. The policies of complete trust and anonymous authorization should be restricted, and the policy of detailed user authorization should be implemented.

Cloud-based Managed Identity and Access Management (IAM) architecture is different from traditional IAM. Security characteristics must include the well-known principles of security viz. confidentiality, integrity and availability. The sample POC framework discussed here is one of the possible ways in which an effective transparent IAM system can be built.

The POC system architecture is shown in Fig. 1, the main components of the system are IAM core – the core IAM functions have been implemented in this module, IAM manager – managerial functions like policy, Identity management etc. have been implemented in this module, on the other side of managed IAM will be protected resources / multiple CSPs. The access to the users will be provided through a web browser.

The implementation has been done in form of a web server running under windows OS Virtual machine in a public cloud setup. The IAM core and IAM manager have been implemented in a separate Virtual machine. The client is first registered and the credentials are stored in MySQL database. The user password is stored in an encrypted form so that it is not visible to anyone not even the Cloud Service Provider. When the user logs in, his/ her credentials are verified and a token is generated which is passed to the protected resources in the private cloud viz. Devices, Data, Application server etc. In this way the entire Identity and Access Management functionality is managed transparently from users and their applications. It is provided as a managed Cloud Service to the client through browser and different types of devices (Desktops and Mobiles devices etc.) can also access it.

4. EVALUATION OF POC MANAGED IAM SERVICE

The evaluation of the POC is done with respect to white paper [9] and papers [10, 11] in which the following criteria have been considered for the evaluation purpose:

- Reliability: the service can be provided in form of multiple web servers running in the cloud environment. The redundancy of servers will lead to high reliability and high availability to the clients. The POC was tested in form of two web servers to provide uninterrupted transparent IAM services to the clients.
- Effectiveness: to make the service more effective, CAPTCHA was also integrated during registration process of the client to protect against Bots and to improve availability.
- Performance: the performance was tested by comparing the average execution time of registration/ login process of managed IAMprovided as cloud service w.r.t. standard legacy IAM for a normal web server. The overall overhead also depends on the traffic in public cloud, but it does not increase by more than 10-15 % (refer Fig 2), which is fairly good given the advantages it offers over legacy systems.
- Flexibility: the solution can work with existing legacy systems as well. Since the POC implementation is in the form of PHP programs it can easily work with legacy IAM systems. It can provide more flexibility to customers to choose varying levels of security as per their need.
- Control: the customer uses a web browser to access the service and it can be accessed from various devices viz. desktops and handheld mobile devices etc.
- Privacy and Security: the protected resources of the customer are inside a private cloud, and access is provided only after successful login. This ensures the privacy and security.
- Cost of ownership: the cost of ownership is borne by the cloud security service provider. The client does not invest in anything in on-premise solution. The client will have to pay only on the basis of pay per use model. Since IAM is available as cloud service it is only charged to customer in form of Operational Expenses (OPEX) model.

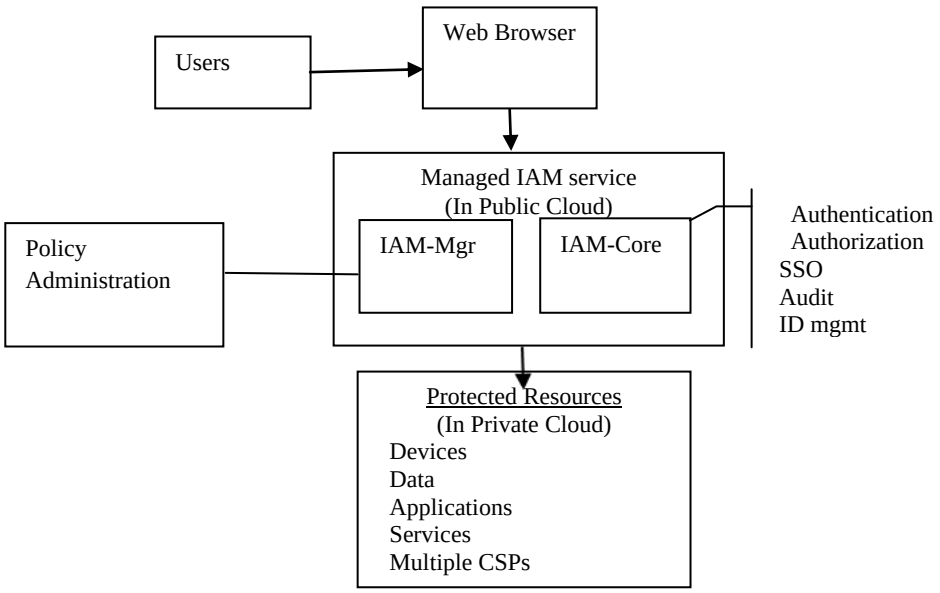
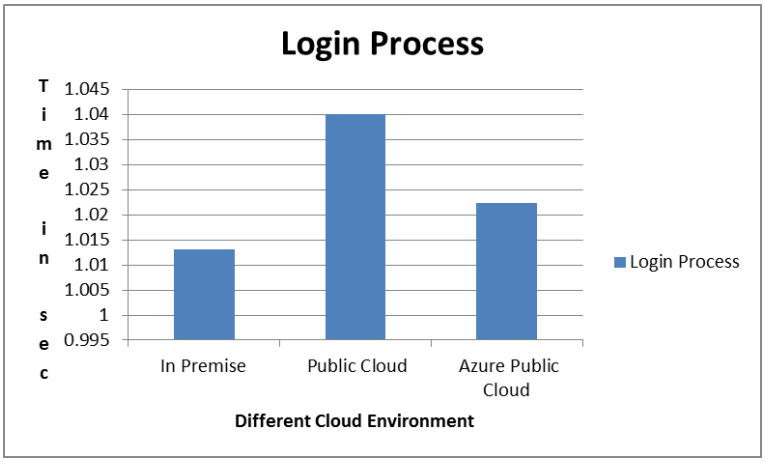


Fig 1: POC for Managed IAM service



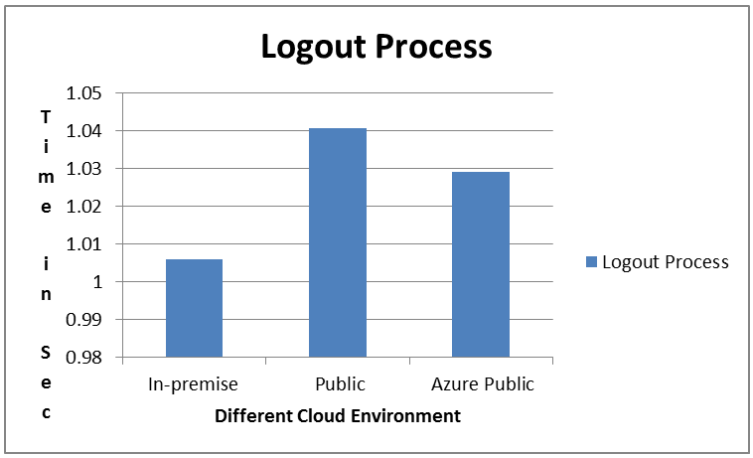


Fig 2: Comparison of Managed IAM Service

5. CONCLUSION AND FUTURE WORK

In this paper, managed transparent IAM service was introduced in the form of a framework that enables the cloud service provider to provide IAM as a cloud service in public cloud. Managed IAM is compatible with prominent cloud features including portability, elasticity, and pay-per-use service. The approach has been implemented transparently as a collection of VMs in cloud environment to comply with the cloud model. This solution can work best with existing on-premise platform based solutions in a hybrid manner to enhance their security capabilities. With managed IAM service, users can define virtual private area with the cloud space for securing their protected resources.

The future work will involve in integrating this POC with various other SECaaS or managed services. The results of the evaluation of POC are encouraging and more IAM services can be added to enhance its functionalities.

6. REFERENCES

[1] Shuai Zhang, Shufen Zhang, Xuebin Chen, XiuzhenHuo, "Cloud Computing Research and Development Trend", 2010 Second International Conference on Future Networks, IEEE 2010

[2] Nicholas Carr,"The Big Switch Rewiring the world from Edison to Google", W.W. Norton & Co. January 2008

[3] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, December 2009.

[4] Cloud Security Alliance, SecaaS Defined categories of service 2011

[5] CSA SecaaS Implementation guide : Identity and Access Management September 2012

[6] Tim Mather, Subra Kumaraswamy, and Shahed Latif, 2009, Cloud Security and Privacy. An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 336.

[7] Samlinson, E.; Usha, M., "User-centric trust based identity as a service for federated cloud environment," in Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on , vol., no., pp.1-5, 4-6 July 2013

[8] Yan Yang; Xingyuan Chen; Guangxia Wang; Lifeng Cao, "An Identity and Access Management Architecture in Cloud," in Computational Intelligence and Design (ISCID), 2014 Seventh International Symposium on, vol.2, no., pp.200-203, 13-14 Dec. 2014

[9] Websense white paper, Seven Criteria for Evaluating Security-as-a- Service Solutions, 2010

[10] Deepak Sharma, Dr. C A. Dhote, Manish Potey, "Security-as-a-Service from clouds : A survey" IIJC Vol 1 Issue 4, October 2011

[11] Deepak Sharma, Dr. C A. Dhote, Manish Potey, "Security-as-a-Service from Clouds: A comprehensive Analysis", IJCA Volume 67-Number 3, April 2013