Identity Management Approach for Software as a Service

Georgiana Mateescu, Marius Vlădescu

Computer Science and Automatic Control Faculty
Polytechnic University of Bucharest,
Bucharest, Romania
georgiana.mateescu@gmail.com, vladescumariusnicolae@yahoo.com

Abstract— **Cloud Computing is defined by flexibility, agility, scalability, reliability – all these being provided using the concept of computing as a utility. Beside all its big advantages, the adoption of the cloud still has a limited number of adherences because it also can expose the consumer to a lot of risks and vulnerabilities, which sometimes are heavier than the benefits themselves. Providing a cloud identity is a key component of a cloud successful story because in such architecture aspects like the request context, sensitive data usage and end-user service availability make the difference between a legitimate and an un-legitimate request. By using several systems that provide only parts of the cloud identity, we ensured that the end user cannot alter his access to cloud application and that the cloud application only manipulate allowed personal data.**

Keywords-Cloud Computing; identity management; Software as a Service.

I. INTRODUCTION

Cloud computing, as defined by National Institute of Standards and Technology (NIST), is a model for enabling always-on, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., storage, applications, services, etc.) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

This definition provides the main characteristics of cloud computing [2]:

- Shared resources – in cloud computing architectures multiple users utilize the same resources from network level, host level to application level.
- Massive scalability – because of its foundation principles, cloud computing has the ability to scale to thousands of systems.
- Elasticity – in cloud computing framework it is very easy to adapt both hardware and software resources to the user's need.
- Pay as you go – cloud computing consumers pay only the resources they use just for the time they actually require them.
- Self provisioning of resources – additional systems (processing capability, software, and storage) and network resources are added when and if they are needed.

These characteristics prove a lot of advantages including: lower-cost computers for users, improved performance, lower IT infrastructure costs for enterprises, fewer maintenance issues, lower software costs, instant software updates, increased computing power, unlimited storage capacity, increased data safety, improved compatibility between operating systems, improved document format compatibility, and universal access to documents [3]. There is also a list of challenges that can be even heavier than the benefits:

- This type of architecture requires constant Internet connectivity; moreover the disconnection can lead to a lot of inconsistencies that can be very hard to clean.
- The services quality is dependent on the connectivity power; it does not matter how strong and reliable a service is; if for bad weather for example, the Internet is slower, the entire performance is compromised
- The data ownership is shared between cloud provider and consumer, which may lead to insufficient security in storing and using the data by the cloud vendor.
- Compatibility issues between the cloud providers can lead to delays in processing data from systems hosted by different vendors, inefficiency in meeting the required Service Level Agreements (SLAs).
- Regulatory compliance issues due to the geographical position of the cloud provider data center.

In order to phase all these challenges, the community proposed standards which came in the help of enterprises and offer them guidelines about what secure architecture means and. Also, from decades of experience, the Internet brought out to light a lot of best practices related to the information security, vulnerabilities, risk assessment and damage management and recovery. In this paper, we will reference the Cloud Security Alliance (CSA) standard that addresses the main security topics within cloud architectures [4].

The first section of this paper presents the actual IT context for cloud computing concept with both its advantages and disadvantages. The second section states the deployment and services models and after this the main security domains together with the challenges from a cloud computing architecture are presented. Identity management within a hybrid company (it uses both on premises applications and on demand services) is the key component that can make the difference between a successful cloud computing story and a failed one. In the fourth section, we propose an approach that addresses the identity management requirements by leveraging the existing architecture within the company. In the last section, before referencing all state-of-the-art cloud computing materials, we conclude with benefits and future work.

 ISBN: 978-1-61208-305-6

II. CLOUD COMPUTING DEPLOYMENT AND SERVICE MODELS

According to Lingenfelter [4], cloud computing is defined by the following characteristics:

- On-demand tenant self-service model for provisioning computing capabilities
- Broad network access and mobile platforms
- Resource pooling through dynamically assigned physical and virtual capabilities delivered in a multi-tenant model and location independent
- Rapid elasticity of provisioned resources
- Measured service to monitor, control and report on transparent resource optimization
- All these features can be delivered as one of the three types of services:
- Software as a Service
- Platform as a Service
- Infrastructure as a Service / Datacenter as a Service

The cloud computing benefits can be implemented using one of the four deployment models depicted in Figure 1.

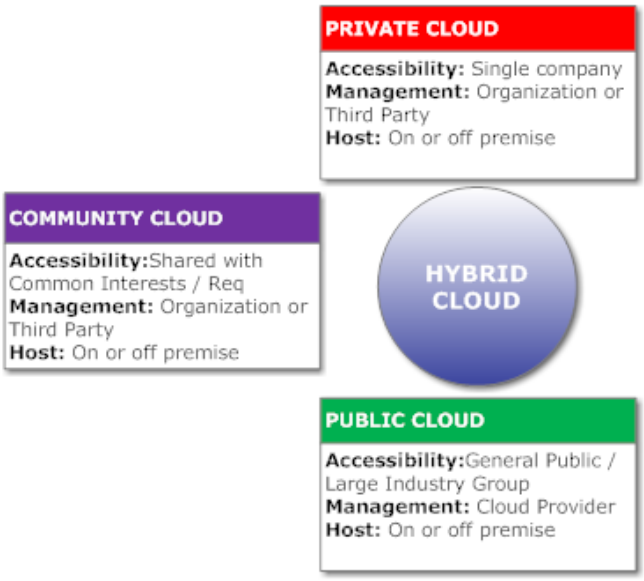

Figure 1. Cloud Computing Deployement Models [13]

The private cloud option is ussualy adopted by companies with multiple braches that choose to maintain all the applications within the organization's firewall having all the benefits the cloud architecture provides.

The community cloud offers the cloud benefits at a community level – a community is a group of organizations that address the same domain of activities. In this model, the cloud services are not kept within firewalls, but are restricted based on community membership.

The public cloud is the least restrictive from access perpective and it has a general use.

Each of these models has certain challenges that lead to the hobrid approch – the combination between private clouds (which usually hosts the most critical application), community clouds (which hosts the applications required for organizations interoperability in every day business process) and public clouds (which hosts applications for general usage – such as customer portals etc.).

Depending on each specific environment and business requirements, the cloud model should be selected after a complex process that involves both technical and functional (business) teams.

III. CLOUD COMPUTING SECURITY CHALLENGES

European Network and Information Security Agency (ENISA) provided a detailed description of all risks that a cloud customer must phase together with the impact and affected areas specific on each risk [2].

When adopting a cloud computing architecture, the company must address a significant number of vulnerabilities and risks including [2]:

- Policy and organizational risks include: Lock-in, Loss of governance, Compliance challenges, Loss of business reputation due to co-tenant activities, Cloud service termination failure
- Technical risks include: resources exhaustion, isolation failure, cloud provider malicious insider – abuse of high privilege role, intercepting data in transit and data leakage on up/download intra-cloud, loss of encryption keys, Economic/Distributed denial of service (EDoS/DDoS)
- Legal risks
- Risks not specific to the cloud include: network management (breaks, congestions, miss-connection, non-optimal use), privilege escalation, backup lost, stolen, unauthorized access to premise, natural disaster
- Vulnerabilities include: AAA vulnerabilities, user provisioning and de-provisioning, remote access to management interface, lack of resource isolation (resources that are used by one customer can affect resources used by another customer), lack of reputational isolation, communication encryption vulnerabilities

In order to efficiently address all these risks and vulnerabilities, CSA categorized all the security aspects from cloud computing architectures into the following domains[4]:

1. Governance and Enterprise Risk Management - The ability to govern and measure risk introduced by cloud computing
2. Legal Issues: Contracts and Electronic Discovery - Security breach disclosure law
3. Compliance and Audit - Evaluate how cloud affects compliance
4. Information Management and Data Security - Managing data stored in cloud
5. Portability and Interoperability - The ability to move data from a cloud provider to another
6. Traditional Security, Business Continuity and Disaster Recovery - How cloud affects the current security procedures

 ISBN: 978-1-61208-305-6

7. Data Center Operations - How to evaluate provider's data center architecture and operations
8. Incident Response, Notification and Remediation - Proper incident detection, response, notification and remediation
9. Application Security - Securing application that runs on different cloud deployment model
10. Encryption and Key Management - Identify proper key usage and key management
11. Identity and Access Management - Cloud-based IdEA (Identity, Entitlement and Access Management)
12. Virtualization - Risk associated with VM isolation, VM co-residence
13. Security as a Service - Third party security assurance including incident management and compliance attestation

In this paper, we will address the Identity and Access Management domain and we will present our approach that leverages the existing Identity Manager system within the company premises in order to accommodate all the cloud specific requirements.

IV. IDENTITY AND ACCESS MANAGEMANT

A. Existing identity management approaches

An Identity Management component is in charge with the following tasks:

- Establish identities: Associate personally identifiable information with an entity.
- Describe identities: Assign attributes identifying an entity.
- Record the use of identity data: Log identity activity in a system and/or provides access to the logs.
- Destroy an identity: Assign expiration date to personally identifiable information. Personally identifiable information becomes unusable after the expiration date.

Identity Management can involve three perspectives [11]:
1. The pure identity paradigm: creation, management and deletion of identities without regard to access or entitlements.
2. The user access (log on) paradigm: A traditional method say for ex a user uses the smart card to log on to a service.
3. The service paradigm: A system that delivers personalized role based, online, on-demand, presence based services to users and their devices.

P. Angin [7] provides an approach to create and manage identities within cloud computing architectures without the need of trusted sources. This approach does not use enterprise systems and it is based on the information stored locally on the machine that attempts to connect to the cloud service.

C. Mitchell [8] describes an identity management mechanism that performs privacy-preserving authentication using anonymous credentials without making usage of any enterprise system.

Waleed Alrodhan [9] provides a browser plug-in approach for user authentication. Every digital identity is a security token. A security token consists of a set of characteristics, such as a username, user's full name, address, SSN etc. The tokens prove that the claims belong to the user who is presenting them. The biggest challenge related to this approach is related to the user behavior: they do not understand the importance of the approval decision or because they know that they must approve the certificate in order to get access to a particular website.

P. Mularien [10] provides a decentralized authentication protocol that helps cloud users to manage their multiple digital identities by providing one set username and password—an OpenID which is further used for cloud authentication. The main disadvantage of this approach is its susceptibility to phishing attacks and social engineering.

Each of the above solutions has its own challenges and risks.

B. Personal approach

In our scenario, we have the following systems:

- On premise Identity Manager system – this system stores all the company employees together with their accounts in the enterprise systems and the access policies that define the systems and services that the users are allowed to use. In order to efficiently implement the access policies, these are configured based on specific employees attributes also stored in the Identity Manager solution. Also this application is the cloud identity issuer that generates the cloud identities based on different components provided by the other applications involved in the authentication process.
- On demand Trusted Certificate store – this system provides digital certificates to the company. Its main task is to verify the digital certificate from the validity, legitimacy and data integrity perspectives.
- On demand cloud services – we used 2 services: Business Intelligence (BI) application and a Customer Relationship Management (CRM) solution

Within a cloud computing architecture, various actors from both on demand and on premises systems are involved in the authentication process. These parties are [6]:
1. Identity Provider (IdP) – this component issues digital identities. In our scenario, the identity provider in the on-premise Identity Manager system and it is a trusted identity store for the cloud services.
2. Service Provider (SP): It provides access to services to the identities that have the right required identities. Our use-case service model in Software-as-a-Service – more specifically we used a Business Intelligence (BI) application and a Customer Relationship Management (CRM) solution.
3. Entity: Entities are the ones about who claims are made. In our scenario, we consider the entity the user himself who wants to access one of the available cloud services.
4. Identity Verifier: Service Providers send them the request for verifying claims about an identity. In our use-case the identity verification is performed using Trusted Certificate Store and it has the particularity that this step is performed by the Identity Provider itself.

 ISBN: 978-1-61208-305-6

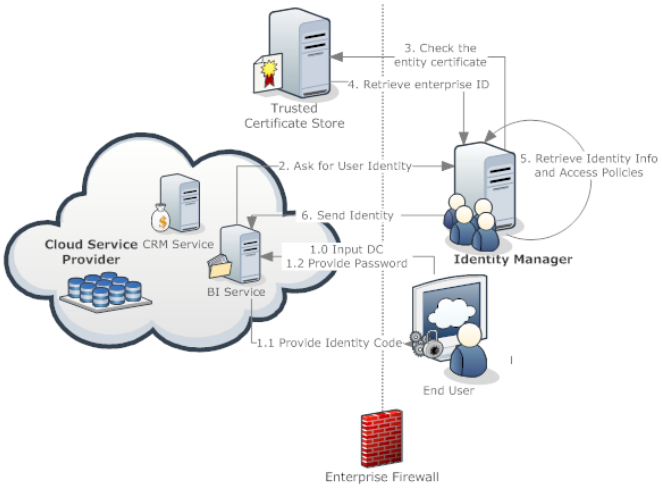

Figure 2. Identity Management Flow

Figure 2 depicts the identity related information flow:

- The user has a token provided by the cloud service provider that generates the password for the cloud service based on a challenge code received from the service provider.
- On the enterprise machine (the user's computer) it is stored a Digital Certificate (DC) that contains, beside the certificate's identifications, the user's enterprise unique identifier and also information related to the device from where the certificate is being used to perform authentication.

The authentication process has the following steps:

1. The user accesses the cloud service and in order to authenticate, he issues the digital certificate.
2. The cloud service answers with a code used by user's personal token to generate the password. The user introduces then the generated password in the service login window.
3. If the password is correct, then the cloud service sends the DC to Identity Manager together with the entity code (the one generated in step 2).
4. Identity Manager sends the DC to the Trusted Certification Store in order to ensure that the certificate is valid and legitimate and to verify data integrity. A certificate is considered *valid* if its expiration date is greater than the day when this authentication request that uses the certification is performed. A certificate is considered *legitimate* if the authentication request that used it, was raised from a host that is allowed to use that certificate. The data integrity is achieved when the personal information of the user stored on the certificate is the same as the one from the store. If all three validations are successfully completed, the Trusted Certificate Store retrieves the enterprise unique id to Identity Manager.

All the data within the digital certificate are encrypted.

5. Using the enterprise unique id, Identity Manager generates the cloud identity based on the specific employee attributes.
6. The Identity Manager encrypts the cloud identity using the key received from the cloud service and sends it back to the service.
7. Based on the allowed accesses for that specific identity, the available services are displayed to the client.
8. After all the activities performed in the cloud service are completed, when the user logs out, the cloud identity is automatically destroyed by the cloud provider.

If any of the validation described in the process fails, then an error is displayed to the user and the access to the cloud services is not granted.

The above presented flow is described from the different systems interactions point of view in Figure 3.

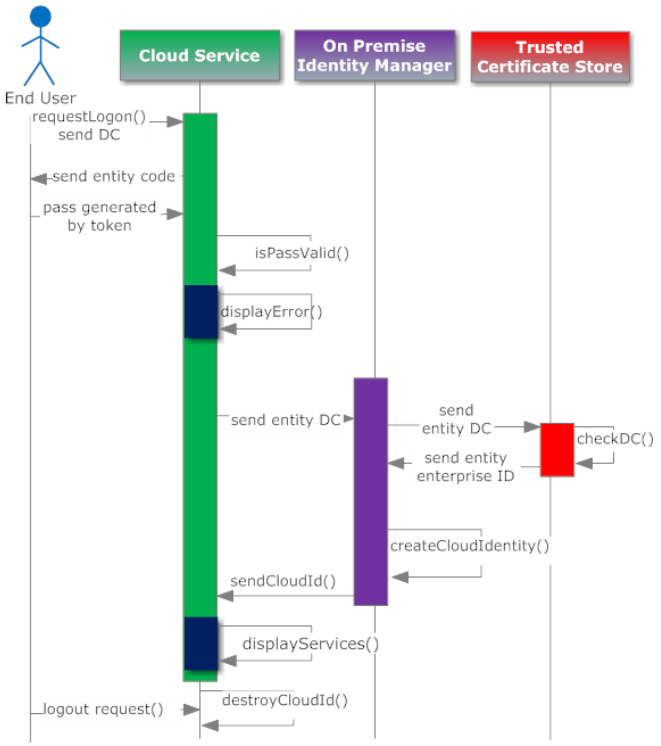

Figure 3. Authentication Process

The cloud identity generated by the Identity Manager system from the enterprise premises contains the following information (Figure 4):

- Personal information about the entity required in order to perform specific tasks in the cloud service that the user is allowed to use (such as fist and last name, personal account, social security number etc).
- Data related rights required to define which operations from the cloud service can use specific cloud identity information (such as the only the payment service can read the account data).
- Access policies required to define which operations from the cloud service are allowed to the user (such as if the user is just a regular user, he is only allowed to purchase some product or to see only his previous transactions).

 ISBN: 978-1-61208-305-6

- Information related to the cloud identify sender – this is used in order to protect against man in the middle attacks, although we considered the communication between the Identity Manager and the Cloud Service trusted (such as the physical address of the computer that made the request to access the cloud service).

In order to protect identity cloud data integrity, we used a symmetric encryption algorithm [12] (the encryption key is the code generated by the cloud service provider in the first step of the authentication).

Figure 4. Cloud Identity

Figure 5 depicts the data usage of the cloud identity within the cloud service:

- The cloud service (Business Intelligence application) decrypts the cloud identity information
- The cloud service (Business Intelligence application) reads from the access policies the services that must be provided to the user
- When the user performs a certain operation, the Business Intelligence application access the personal information according to the data rights from the cloud computing.

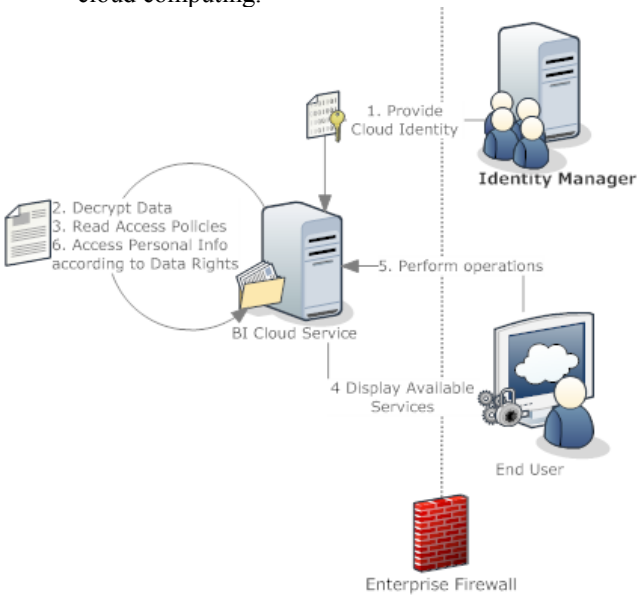

Figure 5. Cloud Identity usage

By using this approach, we managed to control the cloud application user access and also to protect the user data from being used in an abusive manner. The cloud identity ensures that the cloud application will use only the data it is allowed to and that after the access to the cloud application is finished the cloud identity is destroyed.

V. CONCLUSION

According to Jansen and Grance [6], cloud computing guarantees for enhanced performance with lower cost; but, in the same time, the adopters must balance the cost reduction with the security and privacy measures.

In this paper, we presented an identity management approach that allows the enterprises to provide a secure transition step – from on premise architecture to on demand on. This transition supposes a hybrid architecture containing both on premise and on demand systems that interact between each other in everyday business flows.

Providing the fact that on-demand services represent an extension of on-premise applications, existing security techniques can be applied within individual components of cloud computing. We used the on-premise identity provider system to generate cloud identities. This was possible because the identity manager not only stores the identities themselves, but it also has validation and verification capabilities and stores all the policies required to properly set the access to the user.

The main benefits of our approach are:

- The user does not know at any time his cloud identity, thus he will never be able to alter his access rights into the cloud systems.
- The two steps verification process protects against the theft of digital certificate:
  - The first step is the password generated by the token, using the code from the cloud provider – if the attacker steals the DC without having the token, he will not be able to pass the first authentication step
  - The second verification is performed by the Trusted Certificate Store that checks if the certificate issuer is legitimate – this means that even if the attacker managed to steal also the token from the user, if he uses the certificate from another device the authentication process will fail.
- The authentication process involves multiple systems, which means that the man in the middle attack is impossible to be efficiently exploited with a single penetration step.
- The cloud identity contains only the required information according to specific access policies and also data access rights within the allowed services.
- The cloud identity is destroyed after usage, without storing it in the cloud.

Compared to similar papers listed in the beginning of Section IV, we used multiple systems is the identity generation process, fact that minimizes the risk of attacking the identity issuer system. Also, we encrypted the cloud identity data in order to ensure that if it is captured after the entire generation

 ISBN: 978-1-61208-305-6

process is completed, the attacker will not be able to access the data stored in it.

For future works, we plan to address two more areas within the proposed approach:

- The implementation of a more sophisticated encryption algorithm for the cloud identity data
- The single sign on process within on premises and on demand systems.

REFERENCES

[1] Timothy Grance and Peter Mell, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, Sept 2011.

[2] Daniele Catteddu and Giles Hogben, "Cloud Computing Security Risk Assessment", European Network and Information Security Agency (ENISA), 20 Nov. 2009

[3] Jim Reavis , "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0", 14 Nov. 2011

[4] David Lingenfelter, "Cloud Audit and Cloud Trust Protocol", 2011, unpublished, last accessed on October, 5th,2013. https://cloudsecurityalliance.org/research/grc-stack/

[5] Tim Mather, Subra Kumaraswany, and Shahed Latif, "Cloud Security and Privacy. An Enterprise Perspective on Risk and Compliance", O'Reilly United States of America, ISBN-10: 0596802765, 5 Oct. 2009

[6] Wayne Jansen and Timothy Grance , "Guidelines on Security and Privacy in Public Cloud Computing", U.S. Department of Commerce, Special Publication 800-144, December 2011

[7] Pelin Angin, Bharat Bhargava, Rohit Ranchal, Noopur Singh, Lotfi Ben Othmane, Leszek Lilien, and Mark Linderman , "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing", Reliable Distributed Systems, 2010 29th IEEE Symposium, 31 October 2010

[8] Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell : "Policies and Research in Identity Management" - Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013, ISBN 978-3-642-37281-0

[9] Waleed A. Alrodhan and Chris J. Mitchell "Improving the Security of CardSpace", EURASIP Journal on Info Security Vol. 2009.

[10] Peter Mularien, "Opening up to OpenID with Spring Security", May 2010.

[11] Sandeep K. Sood, Anil K. Sarje, and Kuldip Singh, "A secure dynamic identity based authentication protocol for multi-server architecture", Journal of Network and Computer Applications, Volume 34, Issue 2, March 2011, pp. 609-618

[12] Masashi Une and Masayuki Kanda, "Year 2010 Issues on Cryptographic Algorithms", Discussion Paper No. 2006-E-8, IMES, C.P.O BOX 203 Tokyo, 100-8630 Japan

[13] Neeraj Metha, "The 4 Primary Cloud Deployment Models", CloudTweaks, July, 2nd, 2012

 ISBN: 978-1-61208-305-6