WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Safeguarding Data in the Cloud Computing

Shivani[1], Dr. Rupali Ahuja[2]

[1]MTech Student
[2]HOD CSE Department

ABSTRACT:

Many businesses are now considering cloud computing as a means of expanding their current operations. It provides several different types of services to its customers, including IaaS, PaaS, and SaaS. The three pillars of information security—confidentiality, integrity, and availability—will be the focus of this study. Data ownership is a crucial concern for modern enterprises. Authentication, authorisation, and auditing of cloud users are covered in this paper, along with future IAM protocols and standards and cloud-specific security problems.

Keywords- Cloud Computing, Privacy, Security, Identity and Access Management.

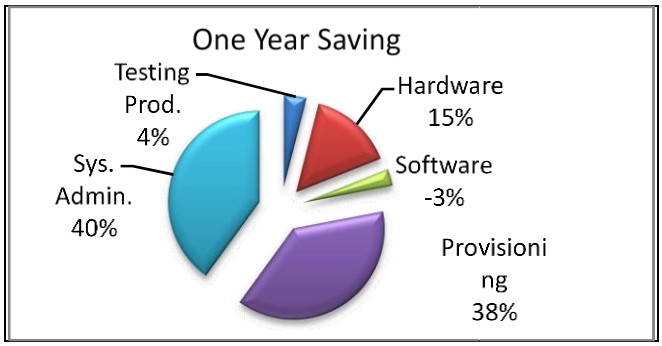
1. Introduction

Understanding cloud computing requires looking back at how technology has evolved through time. Toffler [1] claims to have covered agriculture, industrialisation, and the information era as the three fundamental waves of civilisation. The Information Age has seen several waves, the most recent being cloud computing. Services are delivered via distant servers, or "the cloud." Reduced prices, increased security, and more scalability are the three most important benefits that cloud computing will provide to the market. The major objective of this research is to compare and contrast the various identity and access management (IAM) protocols now in use to protect cloud users, with the end aim of identifying the best options for organisations making the move to cloud service consumption.

According to a study conducted by the IBM group and discussed by Richard Mayo and Charles Perng in [2], most businesses are evaluating the cloud in terms of cost saving tool used regardless of the security provided by the Cloud Service Provider (CSP).

Case study results are shown in Figure 1 for a business that, like a bank, needs many servers to run its operations and, as a result, migrates those activities to the cloud.

Figure 1 Annual Cost-Savings [2]



On page 26 of [3], it is stated that "the US government projects between 2010 and 2015 will increase spending on cloud computing at 40% compound annual rate to $7 million by 2015." This suggests that spending on cloud computing will increase rapidly in the not-too-distant future. One of the primary draws of cloud computing for organisations is the cost savings it may provide. But there are additional challenges that must be considered, such as safety. Businesses are increasingly relying on cloud computing to store and manage data such as databases, user profiles, and even whole IT networks. Is the firm comfortable with the level of security provided by the CSP?

Identity and Access Management (IAM) in the cloud is the area of data security that will be covered in this article. In Section 2, we shall discuss the current structure of cloud computing from a high level. Concerns about privacy and security are addressed in Section 3. In Section 4, we'll look into IAM

issues in depth with an awareness of data security best practises. Protocols and the IAM lifecycle are discussed in Sections 5 and 6. In Section 7 we examine best practises implementing IAM with a cloud service, namely Identity Management-as-a-Service (IDaaS). We conclude in the eighth section.

STRUCTURE FOR COMPUTING IN THE CLOUD

Cloud Computing Architectures

The three main categories of cloud computing are SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).

Let's break these down and examine them one by one:

1) Software as a Service (SaaS): Traditionally, customers have had to purchase a licence and a physical copy of the software before they could install it on their computer and begin using it. However, with SaaS, users pay only for the time they actually spend with the service. While the physical infrastructure is shared across several tenants, each user's virtual space is kept private in a multi-tenant environment [4].

2) Platform as a Service (PaaS) is a service that provides a platform on which software may be built. Developers will make use of the vendor's pre-written code blocks to create their own programme. The system will be web-based and housed in the cloud for easy access.

Similar to conventional "outsourcing" in the business sector, but with significantly fewer costs and effort, providers supply the infrastructure as a service in IaaS by delivering it to the client in the form of technology, datacenters, and IT services [5]. The primary objective is to meet the unique requirements of each customer.

Typical Cloud-Based Services

In this article, we'll look at several popular cloud-based apps and explain why they're useful to end users. When asked why the cloud model is becoming so popular, Rishi Chandra, Google Enterprise product manager, cites "consumer driven innovation changing economics and lowering barriers to entry" [6]. The success of cloud computing relies heavily on user acceptance and satisfaction.

Several articles [8, 9] discuss the usefulness and efficiency of cloud computing. In this paper, we'll take a look at the processes and infrastructures that make possible trustworthy identity management. IAM security relies heavily on adhering to established procedures and norms. The next section of this article will discuss security and privacy for cloud computing, which will shed light on the significance of IAM security in this setting.

Cloud Privacy and Security

Information is not stored on the user's computer but rather in the cloud service provider's servers. After reading this, users may rest certain that their safety is not at risk. In addition, moving to centralised cloud services poses security and privacy risks for consumers, as explained in [4]. During the deployment, there is always a chance that security flaws could surface or that new ones will be found. Secure and private cloud environments are crucial, and they go hand in hand with encouraging interoperability between different cloud service providers. Therefore, we think it's crucial to take a closer look at the safety, privacy, and convenience of cloud storage. Protection of Data in a Three-Tiered System

Connectivity Grade:

When it comes to monitoring network traffic, firewalls, and IDS/IPS, the buck stops with the Cloud Service Provider (CSP).

Host Responsibility:

Critical data may be gleaned from system log files. To monitor when and where programmes have been set up.

Application Scope:

Verifying a program's activity logs, which may be required for digital forensics or incident management.

Protecting cloud data requires meeting stringent security requirements at every level to ensure privacy, reliability, and accessibility.

The Right to Privacy

Keeping consumers' sensitive data safe from prying eyes in the cloud. This may be achieved by the use of suitable encryption techniques that take into consideration the cypher type (symmetric or asymmetric) and other aspects (key length, key management, etc.). The CSP is the one variable that determines the outcome. In [4], MozyEnterprise encrypts customer data, but Amazon S3 does not. It's also useful to be aware of any places where consumers may encrypt their information before sending it in. The CSP is also liable for ensuring that [10] NIST-recommended encryption techniques are actually used.

Honesty:

When using a cloud storage service, users should be concerned not just with data privacy but also with data integrity. While encryption can prevent unauthorised access to data in transit to and from the cloud, it cannot prevent unauthorised changes to data after it has been stored there. Message Authentication Codes (MACs) and Digital Signatures (DSs) are two common methods for ensuring data integrity. In MAC, the data is checked using a sum calculated using a symmetric key. In contrast, the DS approach requires a public key infrastructure (keys that are both public and private). We

believe that Message Authentication Code (MAC) will be the best way to provide the integrity checking mechanism in this case since symmetric algorithms are much faster than asymmetric algorithms. Data integrity is especially important given that PaaS and SaaS have been shown to provide no such security.

Obtainability

A further issue is whether or not the data may be accessed by authorised users upon their request. The best strategy is a preventative one, in which efforts are taken to remove or lessen potential threats to service or data integrity. Identifying potential risks to availability might be challenging. Potential threats to accessibility include network-based assaults, such as Distributed Denial of Service (DDoS) attacks, and CSP availability. Amazon S3 was unavailable for two and a half hours in February 2008, then for eight hours in July 2008.

Our next stop is a comparison of two common methods for authenticating users in the cloud: the Security Assertion Markup Language (SAML) and the Open Authentication (OAuth) protocol.

MANAGEMENT OF IDENTITY AND ACCESS (IAM)

Identity and Access Management (IAM) techniques, such as enforcing login passwords, allocating rights, and creating user accounts, can provide a sufficient degree of security for an organization's resources and data. Guaranteed privacy and security for user data and behaviour extends beyond the bounds of the providing organisation. It will be challenging to maintain track of individual users' identities and guarantee the security of their data given that most businesses rely on many information systems to provide their services.

In addition to managing digital identities, it is also necessary to describe the presence and location of users [5]. These three characteristics are essential for today's technological progress. The term "presence" is most commonly associated with real-time communication systems like Instant Message and Voice over IP (VoIP), where it provides all necessary descriptions of users' status during or after the communication, such as whether the user is idle or active, online or offline, and in some cases providing some specific task the user is performing, such as writing documents or emails. Similar to how persons' locations may be specified by using longitude, latitude, and altitude, an entity's IP address can be used to represent its position.

Problem.

• The largest challenge in identity management is the variety of users an organisation has (consisting of customers, workers, partners, etc.).

• Maintaining a low rate of internal personnel turnover, which varies from business to business and sector to industry based on current market and occupational trends.

Users' identities need to be handled when they are combined or split apart.

Don't let a lot of people share your login info (username, password, etc.).

These challenges, among others, are driving growing interest in centralised, automated identity management solutions among corporations. As such, let's define "identity federation" right now. Businesses in a trust relationship agree to use a standard set of identifiers while conducting business with each other's consumers [4]. The main responsibility will be to keep an eye on how the company regulates access to its external services. Users can access many cloud services with a single login and password using federated Single Sign-On (SSO) systems.

As such, we'd like to discuss the state of the art in identity and access management (IAM), which has been hailed as a boon to businesses and individuals alike for its ability to facilitate authentication, authorisation, and auditing for cloud computing users.

1) Verifying Identity:

The action of proving one's identity to a cloud service. Service-to-service authentication is a method of verifying the identity of a user making a request to access data housed by a third party service.

(2) Permission:

Users can only gain access to protected resources after they have been authenticated. The system will now execute the predefined security procedures.

(3) Auditing:

An audit is a thorough inspection of security-related information to ascertain if it conforms to predetermined criteria. If a security breach is ever uncovered, this will be useful as well.

Preparedness of the Cloud Infrastructure:

A company's information access management (IAM) strategy, structure, and knowledge of the IAM lifecycle must be in good shape before making the move to the cloud.

Choosing a trustworthy identity data source is the first step.

Defining required features of user profiles.

Thirdly, we need to define the current enterprise identity management architecture (whether or not there are isolated active directories connected on the internal network, active directories in the DMZ, and whether or not the company is an id-federation friendly environment where active directories can be accessed by a trusted third party, where deploying federation can be faster and more cost-effective).

Identity providers that support SSO technologies include OpenID, Microsoft CardSpace, and Microsoft Novell Digital Me.

Number five: the Identity Provider's integration with the neighbourhood Active Directory server.

To efficiently manage digital identities, one must first foresee the various states in which a digital identity may exist, and only then provide adequate security for each of those situations. This discussion has inevitably progressed into the realm of the IAM lifecycle. Our next topic will be the different points in time where a digital identity may be used.

I AM LIFECYCLE

It is time to think about the identity in its whole, including all of its conceivable states. Once an identity has been created, used, and deleted, what happens to it is a crucial topic to ask. According to Mather, Kumarasuamy, and Latif [4], the following trend is anticipated for digital identity management.

Stock removal and organisation:

Users will be given the appropriate access roles based on their positions within the company, and these roles will be updated as necessary in the event of a promotion or a demotion. Maintaining an identity's granted access rights involves a lot of manpower, time, and energy. With the right cloud management solutions, such identity Management as a Service (IDaaS), the organisation may be able to sidestep this responsibility.

Authentication and Identity Protection

For a company to create an authentication and authorisation model that is tailored to its needs, it must have access to a centralised authentication and authorisation infrastructure. By putting in place such a strategy, you can be certain that your data and programmes are as secure as possible.

Demand-Driven/Self-Service:

Self-service identity management is a powerful addition to IAM systems. You may now see and update user profiles and reset passwords. access to all of the company's data regardless of where you happen to be.

A Guide to Password Security

Federated Single Sign-On (SSO) systems simplify the process of logging into cloud-based applications. Using a safe method for storing passwords in the cloud, such as MD5 or SHA1 (described in [11] and [12], respectively), is an important part of password management.

Measures for Auditing and Ensuring Compliance:

In this method, possible dangers are identified and stopped by tracking and monitoring access. Monitoring compliance with access control policies may also be aided by conducting audits and generating reports on a regular basis.

PROTOCOL AND STANDARDS OF THE IAM

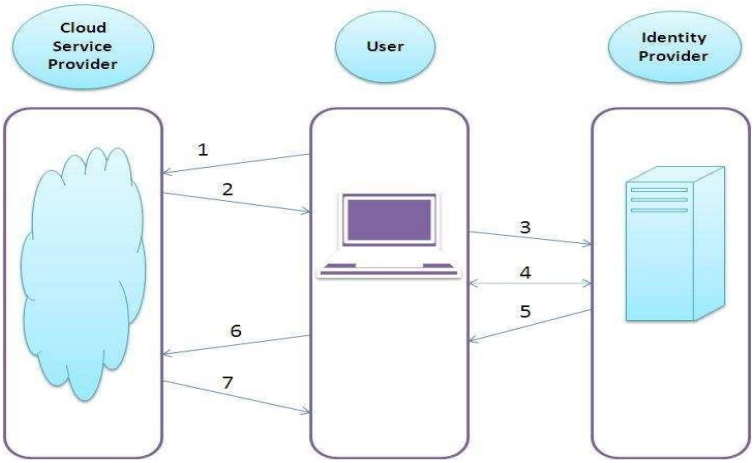
We have previously discussed what is needed to put the IAM structures into place. Below, we'll discuss a few protocols and standards for cloud identity management, but before we do, it's vital to highlight that enterprises and people alike need to put some thought to how they'll make use of IAM protocols and standards.

This piece is dedicated to discussing the company's approach to IAM. Security Assertion Markup Language (SAML) and the Open Authentication (OAuth) protocol are only two examples of the kinds of protocols [4] and standards that businesses should consider using. Here is a detailed explanation of how each of these processes works.

First, we have Security Assertion Markup Language (SAML).

SAML, which is based on XML standards, is used in the cloud as a means of communication between the Identity provider (IdP) and the Cloud Service Provider (CSP) [13]. The fundamental goal of SAML is to offer SSO via the internet. There are currently three different SAML releases from which to choose: 1.0, 1.1, and 2.0. It's possible to digitally sign and encrypt it. For an example of how SAML may be used for SSO between a user, an IdP, and a CSP, consider the following exchange.

Figure: Flowchart of the SAML Exchange Protocol



1. The customer makes initial contact with the CSP to request a website.

2. When a user requests a response from the CSP, it will direct their browser to the IdP's single sign-on (SSO) page.

3. The action of sending a web browser to a new location.

4. Authentication protocols between the IdP and the user are exchanged in the fourth step.

5. The user receives a SAML answer that has been encoded by the IdP.

6. The user's browser will send a SAML response to the CSP in order to visit the URL.

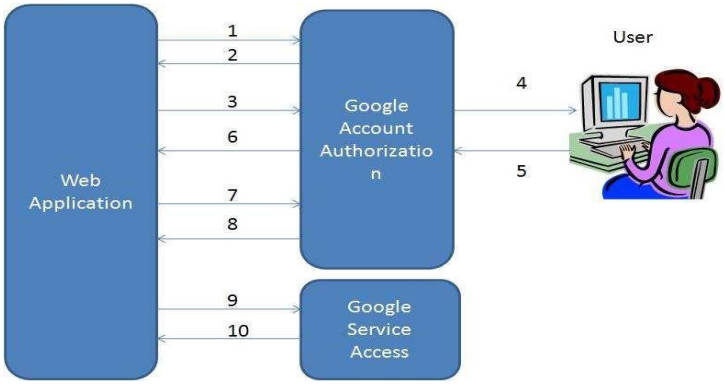
7. The user will be given permission to utilise the CSP application.

Open Authentication Protocol

With OAuth, users don't have to provide sensitive information like login credentials in order to move files, images, and other private resources from one CSP to another [4]. This project's major objective is to provide authorised access to a protected Application Programming Interface (API) that can be integrated into mobile and desktop layouts. From the perspective of the CSP, it provides a service that allows end users to access third-party hosted programmable apps without providing authentication credentials. The consumer (the website or app the user uses to access their files) makes a print service request to the service provider where the file is kept, and the print is made without disclosing the user's credentials.

The OAuth protocol, seen in action in Figure 3 from [4], allows for two-way communication between a user and a service provider.

Figure: Case Study: Using Google OAuth



To begin, the web app must provide a valid OAuth request token to Google.

Google will issue you a "unauthorised request token" if you attempt.

Third, the web app will direct the user to Google's web authorisation page when seeking an authorised token.

The user must first visit the Google Authorisation page to verify their identity and grant or revoke permission for the web application to access their information.

If the user does not grant permission, they will be sent to Google instead of the app's webpage on their browser.

If the user gives their permission, the page will refresh with the application's accepted request Token already embedded in it.

To round up the process, the web app and Google Authorisation will exchange tokens for allowed requests.

Google will issue an Access Token if the request is legitimate.

In order to get information from users, the web app will use Google Authorisation (9).

If the access token is familiar, Google Authorisation will fulfil the request from step 9 and provide the data.

Upon successful authentication, the service provider (in this case Google) will forwards the user to the requested website along with the token received using the OAuth protocol [4]. The cookie contains the token, and the web app may use this to identify the user. The maximum number of tokens an individual user can obtain from a given service provider is subject to change. In order to access the pages you've requested, you'll need an access token, whereas a request token will be needed to actually get an access token from the service provider. Request tokens might be valid or invalid depending on their approval status. When a user successfully signs in, the token they have requested is added to the list of authorised tokens.

WHICH ANSWER IS PREFERABLE?

This statement is highly unclear since the answer relies on how an organisation acts to achieve its business goals. Most CSPs may choose to utilise several authentication techniques to build a more secure security architecture for maintaining their customers' identities, as there is overlap across technologies. SAML is widely used in businesses and schools to allow users single sign-on to a wide range of internal and external services. Due to its extended development history and comprehensive library, SAML is classified as a "Enterprise" digital identity solution. However, it falls within OAuth's "Open Source" library category, which covers libraries that are still in their infancy and might require further protocol development work. We anticipate fierce competition among the OAuth research community. However, SAML is your best chance for implementing federation and SSO in the cloud. Because of its long history and extensive testing against a variety of vulnerabilities and threats, SAML is our top choice for implementing IAM security and safeguarding user data privacy.

Cloud-based I.D. Management as a Service

We may start to contemplate the prospect of outsourcing identity providers via a service like Identity as a Service (IDaaS) now that the cloud has grown to the point where providers may deliver "anything as a service" (XaaS). Many organisations would rather have a third party handle customer and vendor identity management, but they must do it internally for their own staff. This SaaS-based model supports services such as account provisioning, auditing, password management, and user self-services. The architecture allows for full automation of the account creation and verification processes inside an organisation. Several commercially available services, such as Simplified and Ping Identity, provide identity management.

One key perk of outsourcing identity management is access to a multi-protocol environment that supports SAML, OAuth, and more for use with a variety of cloud service federation systems. Users will be authenticated by IDaaS right before logging into any cloud service using browser SSO.

As with any cloud service, this methodology may be easily adapted by any business. One major negative of IDaaS is that it hides the CSP's underlying architecture, implementation, and services from the organisations using it. The produced report on the users may not meet the organization's demand, and the option to modify the report will be constrained by the CSP's capabilities.

SUMMARY

As a result of its low cost and high efficiency, cloud computing presents a tempting environment for the business world. If cloud computing security and privacy issues are addressed, more companies will adopt the technology. IAM must be properly implemented to ensure mutual authentication, authorisation, and auditing for cloud resource management. The major objective of this research is to compare and contrast the various identity and access management (IAM) protocols now in use to protect cloud users, and to identify the best options for organisations making the switch to cloud service consumption.

REFERENCES

[1] A. Toffler, “The Third Wave”, Bantam Publisher , 1984.

[2] Richard Mayo, Charles Perng, “An explanation of where the ROIcomes from”, IBM, November 2009.

[3] “US Federal Cloud Computing Market Forecast 2010-2015”, Tabuler Analysis, Publication, May 2009.

[4] T. Mather, S. Kumarasuwamy and S. Latif, “Cloud Security and Privacy”, O’Rielly, ISBN: 978-0-4596-802769, 2009.

[5] J. W. Rittinghouse,J. F. Ransome, “Cloud Computing: Implementation, Management and Security” CRC Press, ISBN: 978-1-4398-0680-7, 2009.

[6] Paul McDougall, “The Four Trends Driving Enterprise Cloud Computing”,http://www.informationweek.com/cloudcomputing/blog/ archives/2008/06/the-four -trends.html, 10 june 2008, retrieved 26 Feb 2009

[7] M. Dikaiakos, G. Pallis, D. Katsaros, P. Mehra and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research", IEEE Internet Conputing, vol. 13, no. 5, 2009.

[8] "Architectural Strategies for Cloud Computing", Oracle Corporation, August 2009.

[9] H. Cademartori, "Green Computing Beyond the Data Center", © TechTarget, 2007.

[10] L. M. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, vol. 7, no. 4, 2009.

[11] P. Gauravaram, A. McCullagh and Ed Dawson, "Collision Attacks on MD5 and SHA-1: Is this the "Sword of Damocles" for Electronic Commerce?", AusCERT Asia Pacific Information Technology Security Conferenece, pp. 1-13, May 2006.

[12] Z.Y. Hu, ''Password Breaking and Encryption Technology". Machine Industry Press, 1999.

[13] Eve Maler,Scott Cantor, Jahan Moreh, Sigaba,Rob Philpott, "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0", Copyright © OASIS Open, 2005.