ROBUST IDENTITY AND ACCESS MANAGEMENT FOR CLOUD SYSTEMS

Florence Mary Paul David Johnson
fpauldav@student.concordia.ab.ca

Primary research advisor: Dr. Shaun Aghili
Shaun.aghili@concordia.ab.ca

_____

Secondary research advisor: Dr. Pavol Zavarsky
Pavol.zavarsky@concordia.ab.ca

A Project

Submitted to the Faculty of Graduate Studies,
Concordia University of Edmonton

in Partial Fulfillment of the
Requirements for the Final
Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2020

ROBUST IDENTITY AND ACCESS MANAGEMENT FOR CLOUD SYSTEMS

Florence Mary Paul David Johnson

Approved:

Shaun Aghili [Original Approval on File]

Shaun Aghili Date: April 20, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: April 20, 2020

Dean, Faculty of Graduate Studies

Abstract

With increased financial loss and massive data breaches in the cloud-based environments, it is imperative for organizations to invest in new Identity and Access Management(IAM) solutions that are usable and are conforming to all the security requirements needed to protect cloud identities. A robust IAM system acts as a security boundary that controls authentication, authorization and access control for identities and devices both within and outside the organization. This paper explains the requirements of cloud IAM systems and various attacks on them due to weak security controls. The comparative analysis of the technologies and requirements endows an IAM framework aimed at a more integrated approach to secure identities and IAM systems. The framework is achieved by creating a robust algorithm for enhanced assurance levels for identity verification, proofing and continuous monitoring of all cloud identities and activities.

Keywords: Identity proofing, Assurance, Privacy, Authentication, Authorization, Access control, Continuous monitoring.

ROBUST IDENTITY AND ACCESS MANAGEMENT FOR CLOUD SYSTEMS

Introduction

Identity and access management (IAM) entails the management of individual identities, their authentication, authorization, roles, and privileges within or across the organization. Gartner (2019) defines IAM as "the security discipline that enables the right individuals to access the right resources at the right times for the right reasons". IAM is an ongoing process that continuously verifies user identity and enforces access policies each time the user logs on to the cloud application. As organizations adopt cloud services for IaaS, PaaS, SaaS, the identities associated with each of these layers of cloud deployment models also increase. The management of such identities while preserving security, privacy and interoperability have become a complex issue. Single-Sign-On (SSO) and federation are two important concepts used for most cloud-related access. SSO simplifies access to more than one cloud application, by using single login credentials. However, the usage of SSO draws huge attention to cyber attacks. When one cloud application is compromised, all the cloud applications using SSO are at the risk of being compromised.

IAM in the cloud combines identity verification, SSO, federation and complex access policies, which applies the access policy rules continuously for all the applications the user logs in. Cloud IAM is more complex than traditional on-premises IAM since the user access is not defined to any geographical boundary or devices such as Laptop, desktop, In-home devices, Smart devices (Irei, 2019). Numerous IAM solutions and technologies have been adopted by organizations at different layers of the cloud stack, however, identity-related

breaches and cybercrimes continue to increase. This extends to domains like public, government, health, banking, and education.

Major cloud service providers like Amazon, Google and Microsoft have incorporated security features to support authentication, authorization, single sign-on, multi-factor authentication to facilitate secure access to cloud resources. *(Refer to Analysis and discussion of results: Step 2 for the comprehensive list of cloud-based IAM identities, vendors and their features).* Each of the solutions fulfills specific requirements or context depending on the environment and does not completely fulfill all the needed security requirements for a dynamically changing cloud environment. However, a combination of various tools and technologies will help to draft an effective IAM policy.

Cybercrimes are due to the weak security controls which fail to protect the identities and their attributes throughout the identity lifecycle (Bernabe et al., 2019; Werner, Westphal & Westphal, 2017). Furthermore, end users are concerned about how their cloud identities (data, attributes containing PII) are managed and accessed as the users do not have any visibility of the transactions happening at the cloud service provider or the identity provider.

A case to illustrate is the Deloitte, which despite its multi-layered security systems, the hackers were able to infiltrate the global mail server through an administrator account that required one simple password (Tweedie-Yates, 2017). The failure to use multifactor authentication as an added layer of security has enabled the hackers to access the confidential emails and documents which included sensitive personal information. Yet another major breach was Capital One Financial Corporation., the eleventh largest bank in the United States which faced a security misconfiguration of a web application firewall allowing a hacker to gain access to millions of customer credit numbers, credit limits, balances, payment

information stored in cloud servers (Siegel, R. 2019). To cite a few other incidents such as lack of proper identity and access control that prevent or notify the attack immediately as in the case of Amazon S3 bucket's unauthorized access, Facebook's inappropriate use of technologies by using Oauth protocol for authentication which was intended for authorization; failure to use available technology where only 10% of users effectively use second-factor authentication for google services are few examples of identity breaches in the IAM arena.

According to a 2019 midyear data breach report published by Forbes magazine, 3,800 publicly disclosed security breaches resulted in 4.1 billion compromised records over six months (Winder, 2019). Furthermore, an IBM 2019 data breach study estimates the loss of a typical U.S enterprise is $8.19M from a breach; nearly double the global average of $3.92M (Stern, 2019). As such, enterprises are adopting various standards, control frameworks and regulations to achieve a strong IAM system to enhance the security and privacy feature to prevent organizations from data breaches, monetary and reputation losses. The growing incidents of such attacks are compelling the identity solution providers to implement stronger mitigating controls. In addition to the perimeter security of an organization, strong cloud security architecture and strategy (IAM policies) makes the network boundary impenetrable. The security breaches discussed above could have been prevented if a well designed IAM framework is in place and followed diligently. The major identity breaches specific to IAM are shown in Appendix A Table 1.

The research studies the existing features, requirements, and technologies for securing the identities from various identity-related attacks using the IAM systems. For this study, a gap analysis was performed between the security features, mitigated attacks, and the available

IAM related technologies. The findings from the gap analysis were used to achieve the final deliverable to propose a “best in class” conceptual IAM framework aimed at a more integrated approach to secure identity management by creating a robust algorithm for enhanced assurance levels for identity verification, proofing and continuous monitoring of cloud accounts and activities.

The organization of this research paper is as follows: In the ***Introduction*** section, the data breaches and the need for an IAM system to prevent the breaches explaining the problem statement and the research statement are introduced. In the ***literature review*** section, many relevant concepts and facts from various literature studies are discussed, followed by the ***methodology*** section discussing the scope, limitation, research questions, and research deliverable procedures. The next section will be ***analysis and discussion of results*** which explains the steps involved in achieving the research deliverable and explains the achieved conceptual IAM framework. The last section will be the ***results, conclusions, and recommendations*** which discuss the conclusions derived through the research deliverable and best practices to be followed.

Literature Review

The literature review on cloud IAM systems are categorized into five sections namely i) Cloud identity management security challenges ii)Vulnerabilities and Attacks iii) Contribution towards enhancing the security requirements of a robust IAM system iv) Features and requirements of strong IAM system v) Continuous monitoring as a keystone for dynamically changing cloud IAM.

The statements in italics represent the motivation of the proposed research.

Cloud identity management security challenges

Protecting the privacy and security of the identities is important especially when identities are federated. Privacy is directly related to the number of personal information collected from the user and exchanged between the IDP (Identity Provider) and SP (Service Provider). The commonly used federation protocols are Security Assertion Markup Language (SAML) for enterprise organizations and academia federations; Open authentication (OAuth) and OpenID for web applications. The three protocols exchange information in the form of tokens; however, the authentication and authorization process flows are different and have security issues (Mohamed, Hassan, Safdar, & Saleem, 2019). The root-level threat for the federated identity model is due to the lack of strict access control in the database or the database server (Weingartner & Westphall, 2017).

The participants of the federated cloud system collectively enjoy the benefits of each other by sharing the data and resources establishing a circle of trust (CoT). For instance, two companies participating in federation share the identity data in the form of assertions and can still undergo challenges like granting full access to certain resources to the partner company. *Managing and controlling access control of the federation partners is a key challenge in federated cloud environments* (Zefferer, Ziegler & Reiter, 2017). A federated Id is prone to attack and is vulnerable at every login point. This is due to the password being reused for the applications deployed using SSO and federation. The trusted third party in the CoT may not conform to the agreed SLA to protect and secure the data that is shared (Singh & Chatterjee, 2017). Lack of poor cloud security architecture strategy and insufficient due diligence have been on the list of top security threats to cloud computing environment per the recent report from Cloud Security Alliance (Chin, 2019).

Vulnerabilities and Attacks

Habiba, Masood, Shibli, & Niazi (2014) discussed the cloud IAM attacks and security features and *identified a lack of scalable identity proofing in business-to-customer and government-to-citizen deployments in their research.* Mainka, Mladenov, Schwenk, & Wich (2017) analyzed the attacks on SSO protocols and identified two new attacks on OpenID Connect: a. identity-provider confusion, b. malicious-endpoints attack by abusing the gaps in the protocol specification by breaking the security goals of the protocol. The eye-opening findings were reported to authors of the OpenID Connect specification in 2014 to develop a solution. The gap between protocol specification and implementation had several reasons ranging from too complex specifications for implementation to standard developer mistakes and forgotten checks. *The authors proposed Practical Offensive Evaluation of Single Sign-On Services (PrOfESSOS) which is a security Evaluation-as-a Service (EaaS) for SSO. The customizable solution would apply to all existing libraries irrespective of the platform to evaluate the SSO security.*

An assessment of various cloud identity attacks caused by weak security and privacy controls are mapped to NIST 800-53 Rev.5 control family identifiers (NIST, 2020). The weaknesses cause vulnerabilities in the IAM systems and result in data breaches. Table 1 summarizes eighteen possible identity-related attacks due to weak security controls in the IAM system.

Table 1

A mapping between Cloud identity attacks and respective weakness in security and privacy control families from NIST 800-53 Rev.5

Attack Label	Control family from NIST 800-53	Attack Name	Description of the attack
A1	PA-2	User profiling	Whenever the IDP is contacted by the SP, the metadata is shared. This includes the details of the website the user frequently visits, the login attempts and the user activities. The honest but curious SP may use the details from the metadata and could sell the information outside which compromises user privacy (Asghar, Backes, & Simeonovski, 2018).
A2	PA-2, PA-4	Identity propagation	Public IDP like Facebook disseminates user identities to 3rd party applications on-demand. In 2018, the data breach at Facebook shows that the users may release data to one SP at the frontend, but this SP may knowingly or accidentally release the PII to another SP without user consent at the backend.
A3	SC-5	Malicious endpoint attacks	Four possible attacks happen with a broad category under malicious endpoints attack leveraging. They are malicious Discovery service (i) Broken End-User Authentication (ii) Code Injection Attacks (iii) Server-Side Request Forgery (SSRF) (iv) Denial-of-Service (DoS) Attacks (Mainka et al., 2017)
A4	SA-3, SA-4, SI-7	Elevation of privilege	This involves an insider with legitimate access, explicitly raise their access permissions and gain unauthorized access causing financial and data loss.
A5	SC-5	Denial of service (DOS) attack	This attack involves the IAM server being overwhelmed with forged of falsified authentication requests and consumes the resources of the IAM server, thereby the IAM server will not be able to serve a legitimate user request (Habiba et al., 2014).

A6	IA-2(8)(9) SC-23 SI-3(9)	Replay attack	The replay attack happens at the SOAP binding in SAML protocol. The adversary captures the valid identification information and retransmits resulting in unauthorized disclosure of information.
A7	SC-23	Man in the Middle (MITM)	MITM attack may be caused by a logical flaw in the OAuth due to the presence of a malicious IDP or SP. The man in the middle attack is common in both SAML (P-Initiated SSO (POST/Artefact Bindings) process utilizes the SOAP binding) and ODIC flows due to dynamic client registration.MITM also occurs when the SSL connection is not up properly.
A8	IA-12	Identity spoofing	The attacker maliciously manipulating the token during the man in the middle attacks and thereby gaining access to sensitive information. Spoofing can be prevented to a certain level by two-factor authentications.
A9	SC-23	Eavesdropping	This communication level attack can happen in real-time listening of the un-encrypted transactions between the IDP and SP can be intercepted to steal authentication and authorization details and stimulate attacks (Habiba et al., 2014).
A10	MP-5, PE-3(5),SA-10, SA-18,SA-19, SI-7(4)	Data tampering	The integrity of the cloud services is tampered by unauthorized modification of identity data stored at cloud SP or CP during data at rest.
A11	AU-10	Repudiation	When proper security controls are not implemented to track the activity logs in real-time at Cloud IDP or SP, the malicious activity performed by an attacker will not be tracked. This enables the attacker to further repudiate other malicious activities that have been performed at cloud identity servers.
A12	AU-14	Snooping	Snooping is a more sophisticated attack, and uses tools such as keystroke to intercept sensitive information from identity servers in the cloud (Habiba et al., 2014).

A13	AT-2, AT-3	Phishing attack	A phishing attack involves the attacker to acquire the user's PII information and bank account details by forging the user to click a falsified website, which captures all the required details (Habiba et al., 2014).
A14	AC-10, AC-12, AC-17, AU-14, SC-10, SC-23	Session overwriting	The attacker intends to force the client to make use of the attacker's malicious Discovery service. The attacker sets the browser of the user to send two HTTP requests by loading two HTML IFrames time-shifted. The client discovers the malicious discovery service and overwrites the old metadata with the new one malicious metadata and after following the regular IODC protocol flow. The attacker receives the access token and gets access to authorized resources from the SP (Mainka et al., 2017).
A15	MP-5, PE-3(5), SA-10, SA-18, SA-19, SI-7(4)	IDP confusion	The attack happens in OIDC protocol flow, which abuses the lack between the end-user authentication and redemption of received code. Here the attacker modifies the information at phase 2 which is end-user authentication endpoints, which forces the SP sends the access token wrongly to malicious IDP (Mainka et al., 2017)
A16	SC-4	Redirect URI manipulation	Redirect URI Manipulation attack targets the Authentication Request verification that is sent by the IDP. The user victim is redirected to a website controlled by the attacker to gain access to the authorization code initiated by the attacker. An attacker will then be able to log in as any user registered with the IDP to access resources at SP (Mainka et al., 2017).
A17	SC-23	Brute-force attack	The attacker tries various combinations of passwords to gain access to sensitive information. An important reason for this attack is when the IAM server does not comply with the password complexity settings as per the international standards and guidelines (Habiba et al., 2014).

A18	SA-15(5)	API Attacks	Reusable security tokens or passwords, authentication in clear text are some examples of API being threat to cloud IAM. Cloud API's if unprotected are accessible over the internet which gives access to high privileged access to cloud resources.

Note. A1-A18 are the cloud identity attacks mapped with the weakness in security and privacy control families from NIST 800-53 Rev.5

Contribution towards enhancing the security requirements to achieve robust IAM system

For many years, researchers have proposed IAM models for enhanced security, privacy, and trust. The IAM models that are implemented and tested are discussed as part of this literature review in Table 2, explaining with a brief description/benefits, limitations, and scope.

Table 2

Existing working models on IAM

Model	Description/Benefits	Limitation	Scope of research
1. Policy-based identity management schema for managing access in Clouds (Moghaddam, Wieder & Yahyapour, 2017).	Uses semantic analysis of access requests, double authentication, RBAC, match gate to map the access policies to SP. Reliable and scalable IDM to grant access to users, by defining policies.	Research does not address the issue in managing access requests when the number of requests is increased.	Meets the purpose of mapping security requirements of different cloud services with the predefined authentication schemes.
2. PRIMA-Privacy Preserving Identity and Access Management at Internet Scale (Asghar, Backes, & Simeonovski, 2018)	Privacy-preserving, credential-based authentication, with controlled disclosure of user attributes. Prevents active profiling of the users at the IDP, providing controlled disclosure	Computational overhead to calculate the packing attributes at the user's side and verifying the user attributes at IDP increases linearly with the increase in the number of attributes.	To achieve profile unlinkability, selective disclosure, non-impersonation, and deployability
3. Dynamic Federated Identity Management Approach for Cloud-Based Environments (Keltoum & Samia, 2017)	Uses a federated identity management approach for cloud environments to ensure the secure management of identity credentials and eradicate interoperability challenges.	The intermediary federation providers are included as part of the model which enables dynamic federation. The effectiveness and testing of this model have not been discussed.	To achieve agile and dynamic federation to include security, privacy, interoperability, and access rights delegation.

4. Towards Privacy-Preserving and User-Centric Identity Management as a Service (Dash, Rabens, Hörandne & Roth, 2017)	User-centric identity management solution employing proxy re-encryption integrated with OpenID Connect protocol to achieve end-to-end confidentiality, key security, and usability.	Uses a UIM mobile app to generate the re-encryption key, which might not be trustworthy in case of accidental loss of the mobile device. Also, does not provide unlinkability and anonymity.	To achieve privacy by using proxy re-encryption along with user-centricity.
5. Holistic Privacy-Preserving Identity Management System for the Internet of Things (Bernabe, Hernandez-Ramos & Gomez, 2017)	It combines a cryptographic approach for claims-based authentication using the Idemix anonymous credential system, with classic IDM mechanisms by relying on the FIWARE IDM (Keyrock). Provides privacy-preserving, minimal disclosure, zero-knowledge proofs, unlikability, confidentiality, pseudonymity, strong authentication, user consent, and offline M2M transactions.	Transparency, usability, and attribute revocation-aggregation features are partially fulfilled.	To provide privacy-preserving and capability-based access control that has been tailored for M2M interactions in IoT.
6. ARIES: Evaluation of a reliable and privacy-preserving European identity management framework (Bernabe et al., 2019)	Aries framework design integrates privacy-preserving solutions based on Anonymous Credentials Systems (ACS), identity proofing and derivation-methods using physical breeder eID documents, authentication, and Biometric techniques that protect against impersonation attacks, LEAs investigation procedures.	The deployment model involving web browsers which are subjected to web security attacks. Privacy, on the other hand, depends on the segregation of the components and trust level of implementations when each component is handled by a separate organization and implementation does not store data.	To combine technologies to meet the highest level of assurance and prevent identity fraud.
7. Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment (Vo, Fuhrmann, Fischer-Hellmann, & Furnell, 2019)	Privacy-preserving user identity in FIDM to propose Purpose-based Encryption (PBE), to protect the confidentiality of disseminated data with multi-authorities support	The proposal has a limitation on controlling the collusion attacks on the dishonest IDP, SP or malicious host.	To enforce Identity-as-a-Service (IDaaS) as a trusted IAM to preserve the privacy of user Identity.

Note. Brief description/benefits, limitations, and scope of various IDM models

The large-scale cross border identity federations and working groups like eduGAIN, InCommon, Credential, European eiD adopt the best in class technologies and a combination

of protocols by developing, testing and showcasing innovative cloud-based services in areas of e-health, e-Gov, and academia to the community discussed in Appendix D.

Features and requirements of robust IAM system

The selection procedure of the controls selected to mitigate the weakness follow the laws and regulation, data security requirements, and technological controls. The NIST published NISTIR-7874 Guidelines for Access Control System Evaluation Metrics with general guidelines for evaluating access management solutions by focusing on four parameters such as administration, enforcement, performance, and support (NISTIR, 2012). For federated systems, NIST published 800-63-3 Digital Identity guidelines in 2017, as minimum requirements for the federal systems in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions (NIST, 2017). It also provides assurance levels for Identity (IAL), Authenticator (AAL) and Federation (FAL). While on the wire, the SP requests the assertions from the IDP as a single scalar value, for example, if the users are authenticated by multifactor authentication, the authentication policy will be AAL2. Likewise, if the SP demands the federation assertion to be signed and encrypted, then the authentication policy will be FAL2. When sensitive and critical identity details are shared between countries or across the large community, there is a need to enhance the assurance level for authentication and identity proofing.

The selection criteria for each of the assurance levels are given below in Table 3.

The choice of selecting features and requirements of a cloud IAM is a complex task for enterprises and organizations since the attack vectors are unknown and extended through multiple channels, introducing new security challenges.

Table 3

NIST 800-63-3 Assurance Levels

Assurance levels	Description
IAL 1	Attributes are self-asserted
IAL2	An in-person identity proofing is required
IAL3	Attributes verified by CSP through an examination of physical documents
AAL1	Attributes provide some assurance. Requires single-factor authentication.
AAL2	Attributes provide high confidence. Uses two different authentication factors
AAL3	Provides high confidence-same as AAL2, additionally hard cryptographic authenticator for impersonation resistance
FAL1	IDP signs the assertion and sends to SP sing approved cryptography
FAL2	IDP sends signed and encrypted assertion to SP
FAL3	Same as FAL2 along with the user needs to prove the possession of cryptographic key reference in the assertion

Note. IAL=Identity Assurance Level; AAL= Authenticator Assurance Level; FAL= Federation Assurance Level. *Source:* NIST, 2017

Ferdous and Poet (2012) and Tormo, Mármol, and Pérez (2013) cover a broad classification of functional and non-functional requirements that are critical of an IAM system. *In both the works, the authors conclude that the requirements, identification, choice of the security features of an IAM system is an important step in mitigating the identity-related security risks.*

Since the requirements are very fine-grained towards security and privacy, the cloud IAM features are broadly classified as in Figure 1 with further functional mechanisms of each of the features depicted in detail.

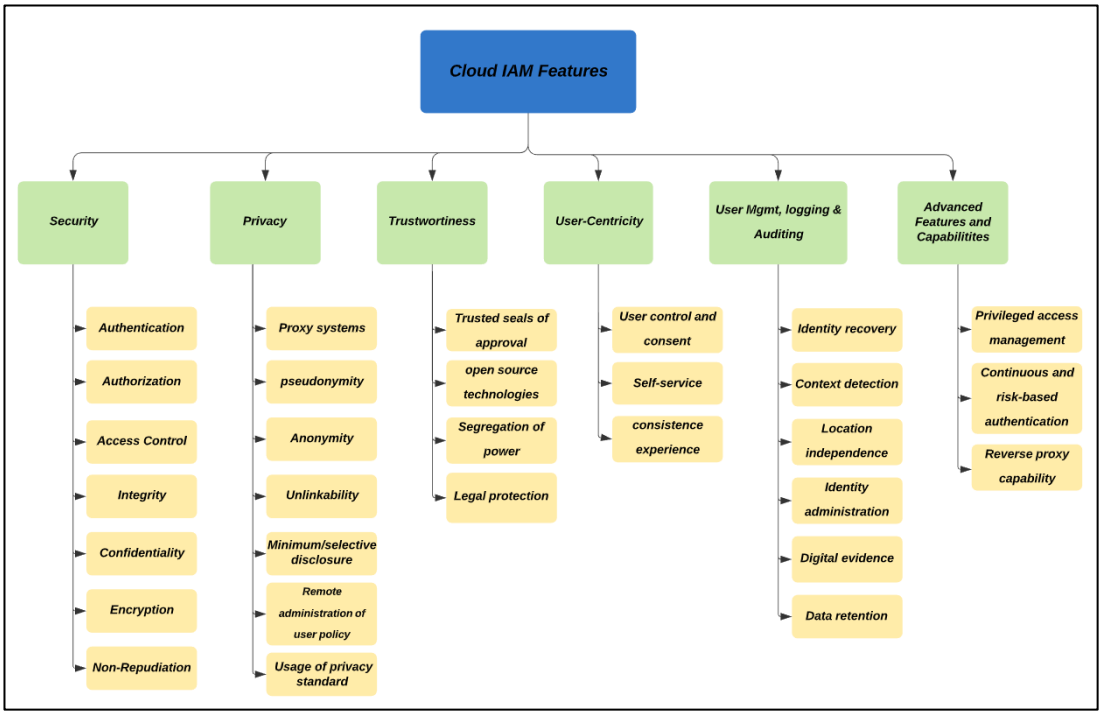

Figure 1. Features and Requirements of IAM systems for the digital era

Continuous monitoring as a keystone for dynamically changing cloud IAM

NIST Special Publication 800-137 "Information Security Continuous Monitoring for Federal Information Systems and Organizations" provides guidelines mentioned in Risk Management Framework (RMF) which states ongoing monitoring is a critical part of the risk management process. NIST SP 800-137 refers to continuous monitoring as: "maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management" (NIST, 2011; Charles et al., 2018). The continuous monitoring evaluates and notifies the effectiveness of the security controls which are continuously monitored to meet the accepted risk tolerance level of an

organization. Additionally, the National Cybersecurity Center of Excellence (NCCoE) is seeking comments on a draft project description to explore continuous monitoring capabilities that can effectively and efficiently detect a malicious actor—be it an authorized user or external actor (Waltermire et al., 2019). The benefits of continuous monitoring and audit are manifold. Continuous monitoring (CM) detects exceptions in real-time through which real-time responses can be provided. CM establishes an automated, risk-based control environment and increases the competitive advantage of the business.

Tep, Martini, Hunt & Choo (2015) and Duncan, Bratterud & Happe (2016) explain the various attacks in the cloud and the possible mitigation strategy and *propose a conceptual architecture for privileged access management in the cloud computing environment that identifies several cloud-specific issues, and its ability to instigate the escalation of user privileges and respond to real-time attacks and argues that continuous monitoring is the only way that the security levels defined by an organization are met.*

Research Methodology

The research focuses on understanding and assessing the security requirements needed for a strong IAM by comparing various security features, underlying technologies, and the mitigated attacks confined to identities in the cloud. The objective is to perform a gap analysis from the available literature reviews and create a “best in class” conceptual IAM framework aimed at a more integrated approach to federated identity management; by creating a robust algorithm for enhanced assurance levels for identity verification, proofing and continuous monitoring of cloud accounts and activities.

The research is limited due to the following reasons: The security requirements and features of traditional on-premises IAM systems are not a new area for study and are not discussed as part of the research since they form the baseline requirement for cloud IAM systems as well. The additional cloud security features discussed as part of this research and the IAM practices make cloud IAM different. Some sections of the research are theoretical, due to the lack of a platform to test the effectiveness of the enhanced assurance levels for authentication. This requires expensive, enormous real-life environments and integration of proprietary identity management tools.

The readers of this paper will find answers to the following questions:

1. What are the major security features and requirements currently available for the prevention of identity attacks in the cloud?
2. How does the achieved integrated framework mitigate security issues and help achieve a strong IAM system in the cloud?

The following steps were taken in building the research deliverable. A study of the cloud security features, requirements and technologies needed for a strong IAM system was conducted from the related works. The various attacks caused by vulnerabilities in the IAM systems that cause data breaches and compromises were accessed. A gap analysis was made by conducting a side by side mapping between the security features, mitigated attacks and available IAM related technologies (protocols). The result of the gap analysis served as a checklist to create a side by side comparison of the respective features and capabilities of the top 4-5 cloud identity solution providers based on market share.

Based on the results of the previous steps, an algorithm for identity verification and proofing based on the Vector of Trust approach (RFC 8485) was created. Additionally, an

algorithm for continuous monitoring of the privileged accounts and cloud admin accounts per NIST 800-53 (guidelines for privileged access AC-6) was created. Finally based on the steps above, a "best in class" conceptual IAM framework has been designed which aims at a more integrated approach to federated identity management towards achieving robust IAM systems.

Analysis & Discussion of Results

The conceptual IAM framework was designed using the five-step process as described in the methodology section. These steps were used to identify the "best in class" security features that are needed for a robust IAM system by identifying the gaps in existing technologies. The final IAM framework is achieved by creating a robust algorithm for enhanced assurance levels for identity verification, proofing and continuous monitoring of all cloud identities and activities. The five steps are discussed in detail below.

Step 1: Conduct a gap analysis by conducting a side by side mapping between the security features, mitigated attacks and available IAM-related technologies (protocols).

A side by side mapping between the security features, mitigated attacks and solution/technologies has been made and presented in Figure 2. The mapping provides a gap analysis of the IAM protocols and/or technologies that are equipped with all the security mechanisms. The given mapping can also serve as guidance for the cloud consumers to understand the features and technology needs of the business and make wise decisions in choosing appropriate cloud IAM solutions. The CSA's Security Guidance for Critical Areas of Focus In Cloud Computing v4.(2017) states that a specific protocol or technology does not

serve magic, whereas the use case of the identities and the constraint under which the IAM system is built should be the primary choice. The protocol should be the second choice.

The results from the mapping show that the identity attacks discussed previously (A1-A18) can be prevented by having the respective security features and mechanisms. The IAM technologies and protocols also fulfill certain security features, mechanisms or contexts depending on the environment and do not completely fulfill all the needed security requirements for a dynamically changing cloud environment. However, a combination of various tools and technologies will help to draft an effective IAM policy.

Feature	Mechanism	Mittigated attacks	CardSpace	Liberty Alliance	Shibboleth	Uprove	Idemix	SAML	XACML	OAUTH	Open ID
Security	Authentication	A4, A5, A6, A8, A9, A11, A13, A17	✓	✓	✓	✓	✓	✓	×	✓	✓
	Authorization	A4, A6, A8, A9, A10, A13	✓	✓	✓	✓	✓	✓	✓	✓	✓
	access control	A3, A4,A8,A10, A1, A17	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Integrity	A3, A7, A8, A10	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Confidentiality	A7, A8, A10,	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Encryption	A1, A2, A9, A8, A10, A13, A12	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Non-Repudiation	A11	✓	✓	✓	✓	✓	✓	✓	✓	✓
Privacy	Proxy systems	A1, A2	×	×	×	×	×	×	✓	×	×
	Use of Pseudonyms	A1, A2	✓	✓	✓	✓	✓	✓	×	✓	✓
	Anonymity	A1, A2	×	✓	×	×	✓	×		×	×
	Unlinkability	A1, A2	×	×	×	✓	✓	×		×	×
	Minimum/Selective disclosure	A1, A2, A4, A8	×			✓	✓	×		✓	✓
	Remote admistration of user policy	A4	×	×	×						×
	Usage of Privacy Standard	A1, A2	×	×	×				×		×
Trustworthiness	Trusted Seals of Approval	-	×	×	×				×		×
	Using Open Source Technologies	A1, A2	×		✓				✓		✓
	Segregation of power	A4	×	×	×				✓		✓
	Legal Protection	-							-		
User-Centricity	User Control and consent	A4, A10	✓	×	×	✓	✓	×	✓	✓	✓
	Self Service	A4	✓	×	×			×			×
	consistence experience	A13	✓	×	×						×
User management,Logging , Auditing	Identity Recovery	A11	✓	×	×						×
	Context Detection	A10, A13	✓	×	×						×
	Location Independence	-	×	✓	✓						✓
	Identity Administration(user account management and Password Management	A10, A15	✓	×	×						✓
	Digital Evidence	A11	×	×	×						×
	Data Retention	A11	×	×	×	×	×	×	×	×	×
Advanced Features and capabilities	Priviledge access management	A4, A7, A10, A17	×	×	×	×	×	×	×	×	×
	Continuous and Risk based Authentication (using adaptive Multifactor and Threat detection using AI)	A4, A5, A7, A8, A10, A11, A14, A15, A17	×	×	×	×	×	×	×	×	×
	reverse proxy capability	A1, A2, A8, A10	×	×	×	×	×	×	×	×	×
Supprting companies								Oracle, IBM,Novell computers Microsoft, Ping Identity, Centrify, VeriSign	Oracle, IBM,Novell computers,CISCO,Red Hat	Google, Twitter,Facebook,IBM, Microsoft, NRI, PingIdentity, Layer 7	Google, IBM,Microsoft, yahoo,paypal,Verisign,AOL, NRI, Ping Identity, Layer 7

Figure 2. A mapping between the security features, mitigated attacks and solution/technologies

Readers interested in reviewing the full list of the mappings may retrieve it at Google doc address: https://docs.google.com/spreadsheets/d/1Ogl_nelTuoomM2A5ArAwRzLCwc-lFoiMvC-2ocidgIw/edit?usp=sharing

Step 2: Perform a side by side comparison analysis of the respective features and capabilities of the top 4-5 cloud identity solution providers based on market share.

Adopting a cloud-based Identity-as-a-Service (IDaaS) and cloud IAM solutions become a logical step to manage cloud identities. Cloud providers offer IAM services to manage identities of cloud administrators in the organization as well as offering customer IAM services to manage identities of the end-users, whether they are external customers or its employees. Tables 4 and 5 provide the list of major cloud infrastructure providers as well as third-party providers offering such services.

Table 4

Cloud provider identity services and customer identity management system

Provider	Cloud identity system	Customer identity management system
Amazon Web Services	Amazon IAM	Amazon Cognito
Microsoft Azure	Azure Active Directory B2C	Azure Active Directory B2C
IBM Cloud	Cloud IAM	Cloud Identity
Auth0	-	Customer Identity Management
Ping	-	Customer Identity and Access Management
Okta	-	Customer Identity Management
Oracle	-	Oracle Identity Cloud Service
Google Compute Cloud	Cloud Identity	Firebase

Note: Major cloud providers and their solutions

Table 5

Top IAM Solution Providers

Solution Providers	Overview	Features	Delivery
Microsoft Azure Active Directory	Integrates with on-premises Active Directory	Multi-tenant feature, Conditional access, RBAC, SSO, MFA, role management, security & user monitoring	Cloud
IBM Security Identity and Access Assurance	Provides IAM and governance across extended enterprises	SSO, MFA, log management, compliance, identity federation, onboarding	Cloud, on-premises

Oracle Identity Cloud Management	Provides IAM for employees, partners, and customer across hybrid environments	SSO, MFA, compliance, integrated directory solution	Cloud
Okta	IAM and mobility management for employees, partners, customers	RBAC, SSO, MFA, Universal Directory, compliance, unified management, activity monitoring, API access management, Platform independent	Cloud, on-premises
Centrify	Manage access across applications, devices, and environments	SSO, MFA, compliance, activity monitoring, mobile management	Cloud, Mobile
Sail Point ldentitylQ	Integrates IAM across cloud, mobile, on-premises	SSO, MFA, compliance, activity monitoring, role management	Cloud, on-premises
Ping	Integrates users, networks, devices, and apps	SSO, MFA, directory, governance, user portal, thousands of supported apps	Cloud, on-premises
ForgeRock	Integrates IAM across cloud, mobile, on-premises	SSO, User provisioning, Auditing, and Reporting, Identity Synchronization	Cloud, on-premises
HID Global	Provides citizen identity and advanced authentication services	MFA, Secure physical and logical access, Analytics and reporting	Cloud, on-premises

Note. List of top IAM products as of use case and features arranged as per market share. Source:10 Top IAM Products, 2017

Step 3: Formulate an algorithm to achieve enhanced identity assurance levels for identity verification and proofing using the Vector of Trust approach (RFC 8485) based on the results of the previous steps (1,2 and 3).

A practical and convincing approach called “Vector of Trust (VoT)” RFC 8485 was introduced by Justin and Richer and Leif Johansson’s that measures the trust of the credentials using multiple scales during the transaction by using Level of assurance (LoA) and Attribute-based access control (Richer & Johansson, 2018). Rather than having a single scalar value, VoT has four different scales based on four orthogonal components that convey

a specific level of identity and authentication proofing and ranks them from Low to High, depicted in figure 3.

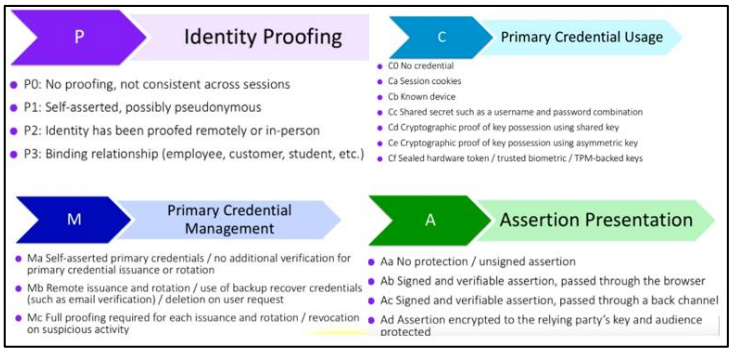

Figure 3. Components of Vector of Trust. Source: Edwards, 2017(RSA Conference)

VoT determines how a user account is proofed, credential usage, credential management, and assertion traversal. When an assertion is exchanged, i.e. when the user contacts the IDP, the IDP measures the trust level of the user by asserting all the vectors at a time (E.g. P1.Cb.Cc.Ma). When all the factors are verified, the IDP authenticates the user and sends the assertion to the SP for authorization. The main objective of enhancing the verification levels to authenticate users of high-risk and high-assurance systems like federal and regulated environments will be fulfilled by this approach. The LoA details are added to the federation metadata files, where the SPs trusting the federation operator can rely on the correctness of the provided IDP, thus enabling high assurance to an authenticated user (Hommel, Grabatin, Metzger, & Pöhn, 2016).

The algorithm to achieve enhanced identity assurance levels for identity verification, proofing is given below:

Step 1: SP will announce which LoA is allowed or acceptable based on its requirements.

Step 2: The IDP‘s will also have their LoA defined and declared. The IDP will assert each user based on their agreed LoA and the assertion will be encoded and sent as a SAML /OIDC assertion token from the IDP to the SP.

Step 3: Figure 4 shows a sample OpenID token requiring pseudonyms, proof of shared key, signed back-channel verified token, and no claim made toward a credential. By using the "vot" and "vtm" values inside the ID token, the vector and its context are strongly bound to the credential represented by the ID token

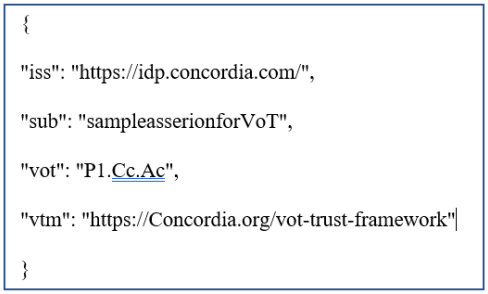

Figure 4. A sample OpenID token with VoT assertion

Step 4: Formulate an algorithm for continuous monitoring of the privileged accounts and cloud admin accounts per NIST 800-53 using guidelines for privileged access AC-6

Figures 5, 6 and 7 check the feasibility of continuous monitoring of privileged accounts using PowerShell by creating accounts in **Azure AD** (portal.azure.com) which periodically monitors the members of Enterprise admins, schema admins, domain admins, cloud admins in specific. *This illustration shows that additional internal control can be added to any IAM system* (AWS cloud or Google cloud irrespective of the scripting languages) *to enable continuous monitoring of cloud accounts, databases or activities.*

A similar kind of automation has been implemented in Active directory which continuously monitors the privileged groups. The PowerShell script is executed every five

minutes to check if the group membership has changed. This functionality can be leveraged to check if any database or servers are subjected to unauthorized access by querying the log files (Constantinou, 2018).

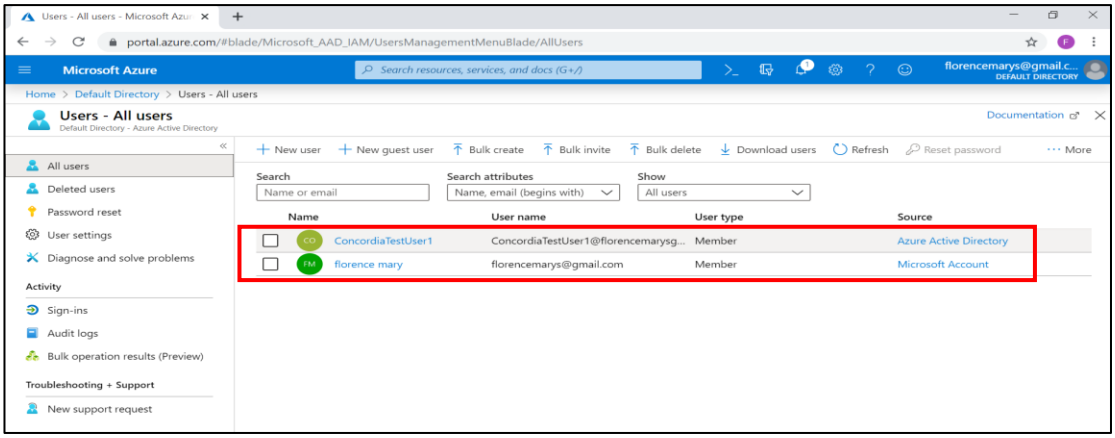

Figure 5. Test cloud user account creation

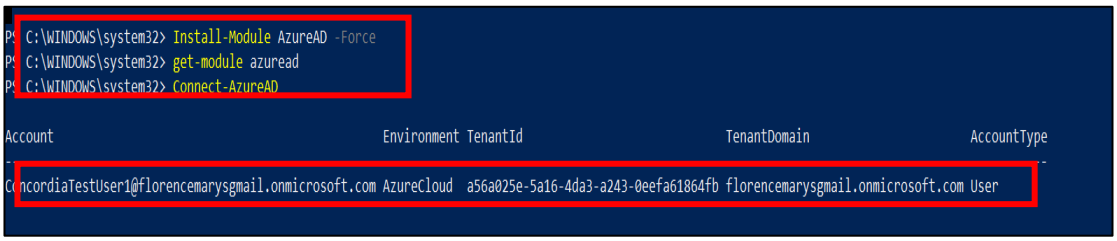

Figure 6. Importing modules and connect to cloud interface to display cloud users

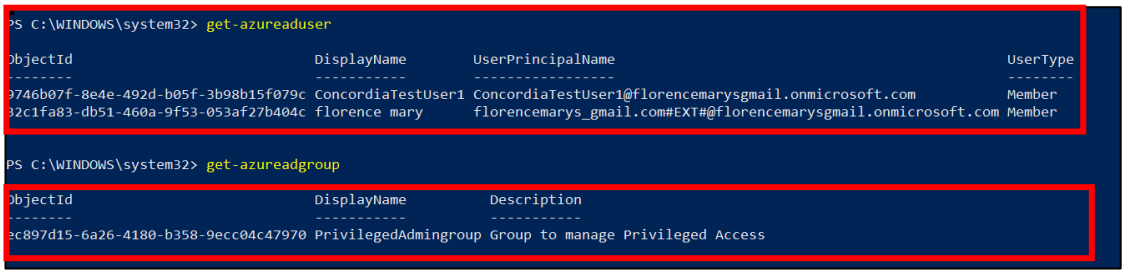

Figure 7. Display Privileged Groups

Algorithm/flowchart to monitor the privileged accounts/databases/containers

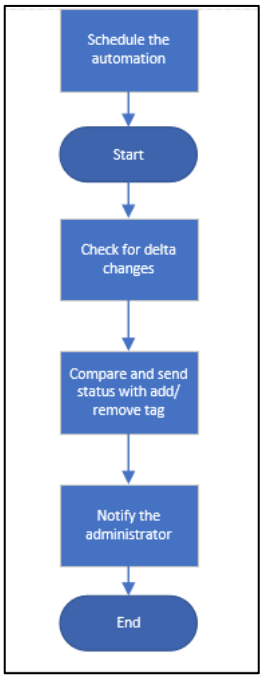

Figure 8. Process flow to achieve continuous monitoring

Step 5: Proposal for a "best in class" conceptual IAM framework for enhanced cloud security

This section aims to show a more integrated approach to identity management towards achieving robust IAM. The framework is built using a seven-step process, adapted from the Risk Management framework for Continuous Monitoring which covers the NIST best practices to manage the information security and privacy risks (NIST, 2018).

Step1 - **Categorize** Information System: The inventory and scope of the identities and devices under the cloud context are identified and classified based on business needs.

Step 2- **Select** security controls and policies: The results from the gap analysis, listed various security controls that are required from the cloud environment in addition to the baseline

security controls. The security controls and policies are selected based on the requirement, technology, and cloud platform.

Step 3 - **Implement** security controls and policies: The selected security controls with six features and thirty mechanisms are carefully implemented.

Step 4 - **Assess** security control and policies: The implemented security controls are evaluated and assured that they are implemented

Step 5 – **Authorize** information systems: The administrator authorizes and allows the security policy to be applied to the identified identities/devices/environment

Step 6 – **Continuous Monitoring** of security controls: The implemented security controls are monitored in real-time

Step 7 – **Implement** corrective actions: Perform corrective actions based on any deviations found from the real-time monitoring.

All the above steps follow *Continual Service Improvement(CSI)* which updates and improves itself at every step. The conceptual IAM framework to achieve a robust cloud IAM shown in Figure 9.

The conceptual IAM framework can be retrieved at Google doc address:

https://docs.google.com/spreadsheets/d/1Ogl_nelTuoomM2A5ArAwRzLCwc-lFoiMvC-2ocidgIw/edit?usp=sharing

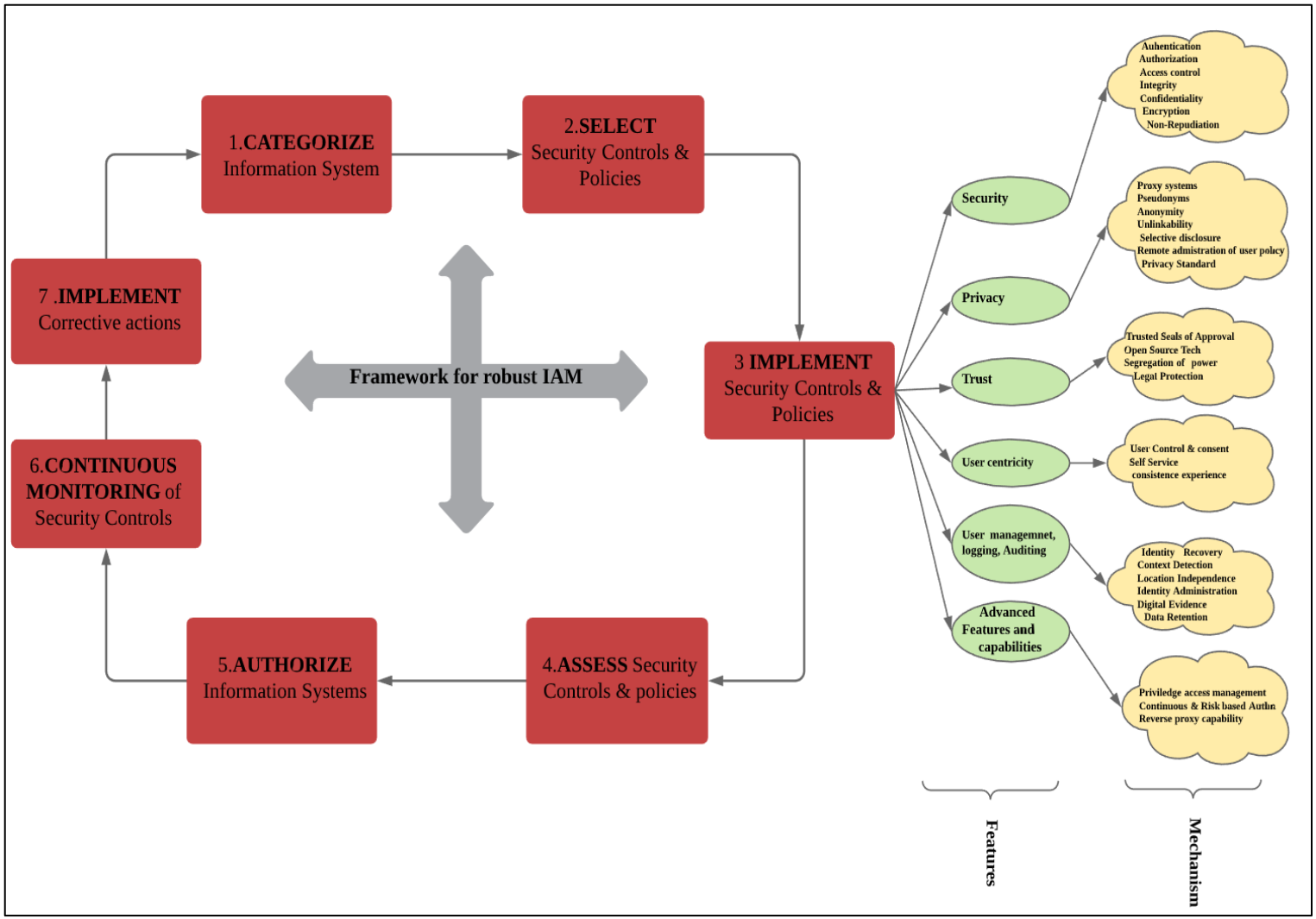

Figure 9. Conceptual IAM framework for robust IAM

Recommendations, Results, and Conclusion

The key to business success lies in understanding what the IAM means to the cloud context and developing a future-ready IAM strategy and framework to protect digital identities. Knowing what identities or devices to protect, understanding the shared responsibility model of the cloud, and knowing the service level agreements add value to create a robust IAM framework. As part of the study, eighteen different identity attacks against the cloud IAM systems have been categorized from various literature reviews and appropriate security features that prevent the attacks are identified (Table 1 and Figure 2). A combination of few to many security features in an IAM system will help mitigate the cloud identity attacks based on the use cases and requirements.

The related works discussed so far have three significant shortcomings. Firstly, the related works are focused on enhancing only a few security features that fulfill the goals partially to build an IAM system. Secondly, little to less contribution is done in the area of enhancing the usability of LoA, where mapping the different LoA in high-assurance domains seems to be a very complex issue. Thirdly, identity governance and monitoring are now purchased as a separate product integrated into an IAM system. On the contrary, these shortcomings can be overcome by implementing continuous monitoring coupled with AI and data analytics in an IAM system. This will detect the incidents proactively and secure the identities from various cyberattacks.

In conclusion, it is clear from the above discussions, the concept of enhanced assurance levels for identity verification /proofing and continuous monitoring has not been addressed in any literature review so far. The integrated IAM framework provided

in this research paper combines both continuous verification and monitoring which is constantly improved for updates and changes in real-time and would help achieve a robust cloud IAM system.

The IAM framework achieved with this work is suited for critical domains involving the federal and health sector where identity proofing and assurance of employees or users of the domain are tested upon. The framework can still be applied with required adjustments to the identity proofing depending on the organization's requirements on authenticating a user.

As future work, the conceptual IAM framework can be integrated into a real IAM platform to test the robustness of an IAM system. It is also worth adding a decentralized identity model using blockchain in future studies.

References

10 Top IAM Products. (2017). Retrieved from https://www.esecurityplanet.com/products/top-iam-products.html.

2019 Data Breaches: 4 Billion Records Breached So Far. (2019). Retrieved from https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html#ent.

Alansari, S., Paci, F., Margheri, A., & Sassone, V. (2017). Privacy-Preserving Access Control in Cloud Federations. 2017 IEEE 10th International Conference on Cloud Computing (CLOUD). doi: 10.1109/cloud.2017.108

Asghar, M. R., Backes, M., & Simeonovski, M. (2018). PRIMA: Privacy-Preserving Identity and Access Management at Internet-Scale. 2018 IEEE International Conference on Communications (ICC). doi: 10.1109/icc.2018.8422732

AWS Best Practices (2016). Retrieved from https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

Barreto, L., Scheunemann, L., Fraga, J., & Siqueira, F. (2017). Secure storage of user credentials and attributes in federation of clouds. Proceedings of the Symposium on Applied Computing - SAC 17. doi: 10.1145/3019612.3019627

Bernabe, J. B., David, M., Moreno, R. T., Cordero, J. P., Bahloul, S., & Skarmeta, A. (2019). ARIES: Evaluation of a reliable and privacy-preserving European identity management framework. Future Generation Computer Systems, 102, 409–425. doi: 10.1016/j.future.2019.08.017

Bernabe, J. B., Hernandez-Ramos, J. L., & Gomez, A. F. S. (2017). Holistic Privacy-Preserving Identity Management System for the Internet of Things. Mobile Information Systems, 2017, 1–20. doi: 10.1155/2017/6384186

Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., & Garcia-Blas, J. (2018). Federated Identity Architecture of the European eID System. IEEE Access, 6, 75302–75326. doi: 10.1109/access.2018.2882870

Charles, K., Eisen, O., Hollebeek, T., Sotnikov, I., Jennings, R., & Richi Jennings. (2018, November 3). Continuous Monitoring: Academic Paper. Retrieved from https://securityboulevard.com/2018/11/continuous-monitoring-academic-paper/.

Chin, V. (2019). Egregious 11 Meta-Analysis Part 1. Retrieved from https://cloudsecurityalliance.org/blog/2019/08/13/egregious-11-meta-analysis-part-1-insufficient-due-diligence-and-cloud-security-architecture-and-strategy/

Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. (2017). Retrieved from https://cloudsecurityalliance.org/download/securityguidance-v4/.

Complete Identity and Access Management Solution (2019). Retrieved from https://www.identityautomation.com/.

Dash, P., Rabens, C., Hörandne, F., & Roth, S. (2017). Towards Privacy-Preserving and User-Centric Identity Management as a Service. L. Fritsch Et Al. (Eds.): Open Identity Summit 2017, Lecture Notes in Informatics (LNI), Gesellschaft Für Informatik

Diniz, T., Felippe, A. C. D., Medeiros, T., Silva, C. E. D., & Araujo, R. (2015). Managing Access to Service Providers in Federated Identity Environments: A Case Study in a Cloud Storage Service. 2015 XXXIII Brazilian Symposium on Computer Networks and Distributed Systems. doi: 10.1109/sbrc.2015.32

Duncan, B., Bratterud, A., & Happe, A. (2016). Enhancing cloud security and privacy: Time for a new approach? 2016 Sixth International Conference on Innovative Computing Technology (INTECH). doi: 10.1109/intech.2016.7845113

Edwards, J. (2017, March 13). Measuring Authentication: NIST 800-63 and Vectors of Trust, A Presentation. Retrieved from https://solutionsreview.com/identity-management/measuring-authentication-nist-800-63-and-vectors-of-trust-a-presentation/

Esposito, C. (2018). Interoperable, dynamic and privacy-preserving access control for cloud data storage when integrating heterogeneous organizations. Journal of Network and Computer Applications, 108, 124–136. doi: 10.1016/j.jnca.2018.01.017

Ferdous, M. S., & Poet, R. (2012). A comparative analysis of Identity Management Systems. 2012 International Conference on High-Performance Computing & Simulation (HPCS). doi: 10.1109/hpcsim.2012.6266958

Gartner Magic Quadrant for Access Management (2019). Retrieved from https://www.gartner.com/doc/reprints?id=1-1ODVSNIK&ct=190813&st=sb.

Gebel, G., Kemp, T., & Mehta, N. (2013). Understanding and Selecting Identity and Access Management ... Retrieved from https://securosis.com/assets/library/reports/Understanding_IAM_For_Cloud_Full.pdf.

Gonzalez, N. M., Rojas, M. A. T., Silva, M. V. M. D., Redigolo, F., Tereza Cristina Melo De Brito Carvalho, Miers, C. C., Ahmed, A. S. (2013). A Framework for Authentication and Authorization Credentials in Cloud Computing. 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. doi: 10.1109/trustcom.2013.63

Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1). doi: 10.1186/s40294-014-0005-9

Haddouti1, S., & Dafir Ech-Cherif El Kettan, M. (2015). Towards an Interoperable Identity Management Framework: a Comparative Study. IJCSI International Journal of Computer Science Issues, 12(6).

Hommel, W., Grabatin, M., Metzger, S., & Pöhn, D. (2016). Level of Assurance Management Automation for Dynamic Identity Federations based on Vectors of Trust. PIK - Praxis Der Informationsverarbeitung Und Kommunikation, 39(3-4). doi: 10.1515/pik-2016-0003

Identity Management - Access Management - Gartner Research. (2019, September 3). Retrieved from https://blogs.gartner.com/it-glossary/identity-and-access-management-iam/

Irei, A. (2019). New tech steers identity and access management evolution. Retrieved from https://searchsecurity.techtarget.com/feature/New-tech-steers-identity-and-access-management-evolution

Keltoum, B., & Samia, B. (2017). A dynamic federated identity management approach for cloud-based environments. Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing - ICC 17. doi: 10.1145/3018896.3025152

Mainka, C., Mladenov, V., Schwenk, J., & Wich, T. (2017). SoK: Single Sign-On Security — An Evaluation of OpenID Connect. 2017 IEEE European Symposium on Security and Privacy (EuroS&P). doi: 10.1109/eurosp.2017.32

Martin, J. A., & Waters, J. K. (2018, October 9). What is IAM? Identity and access management explained. Retrieved from https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: Beijing: Oreilly, Inc

Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2017). A policy-based identity management schema for managing accesses in clouds. 2017 8th International Conference on the Network of the Future (NOF). doi: 10.1109/nof.2017.8251226

Mohamed, M. I. B., Hassan, M. F., Safdar, S., & Saleem, M. Q. (2019). Adaptive security architectural model for protecting identity federation in service-oriented computing. Journal of King Saud University - Computer and Information Sciences. doi: 10.1016/j.jksuci.2019.03.004

National Institute of Standards and Technology (NIST). (2011).Special Publication 800-137. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

National Institute of Standards and Technology (NIST). (2017).Special Publication 800-63-3. Digital Identity Guidelines.Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

National Institute of Standards and Technology (NIST). (2018). NIST SP 800-37, Revision 2. Risk Management Framework For Information Systems And Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Institute of Standards and Technology (NIST). (2020). Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf

National Institute of Standards and Technology Interagency Report 7874 (NISTIR). (2012). Guidelines for Access Control System Evaluation Metrics. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7874.pdf

Richer, J., & Johansson, L. (2018). Vectors of Trust. Retrieved from https://tools.ietf.org/html/rfc8485

Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0. (2005, March). Retrieved from https://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.

Security Guidance for Critical Areas of Focus In Cloud Computing v4.0. (n.d.). Retrieved from https://cloudsecurityalliance.org/download/security-guidance-v4/

Siegel, R. (2019, July 30). Capital One looked to the cloud for security. But its own firewall couldn't stop a hacker. Retrieved from https://www.washingtonpost.com/technology/2019/07/30/capital-one-looked-cloud-security-its-own-firewall-couldnt-stop-hacker/

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88–115. doi: 10.1016/j.jnca.2016.11.027

Siriwardena, P. (2017, September 3). The Role of Identity and Access Management in the Era of Digital Transformation. Retrieved from https://medium.facilelogin.com/the-role-of-identity-and-access-management-in-the-era-of-digital-transformation-48a472ce3247

Stern, R. A. (2019, September 10). IBM/Ponemon Institute 2019 Cost of a Data Breach Report Shows Cybercriminals Continue to Exact Significant Financial Impact on Organizations. Retrieved from https://www.lexology.com/library/detail.aspx?g=0ec5070e-0e81-4621-baec-b9e6d4b0f04c

Constantinou, S. (2018). Get Group Membership Changes. Retrieved from https://gallery.technet.microsoft.com/scriptcenter/Get-Group-Membership-a20a5c95

Tep, K. S., Martini, B., Hunt, R., & Choo, K.-K. R. (2015). A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management. 2015 IEEE Trustcom/BigDataSE/ISPA. doi: 10.1109/trustcom.2015.485

TerryLanfear. (2019). Security best practices and patterns - Microsoft Azure. Retrieved from https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

Tormo, G. D., Mármol, F. G., & Pérez, G. M. (2013). Identity Management in Cloud Systems. Security, Privacy and Trust in Cloud Systems, 177–210. doi: 10.1007/978-3-642-38586-5_6

Tweedie-Yates. (2017, December 8). How Poor Identity Access Management Equals Security Breaches. Retrieved from https://auth0.com/blog/how-poor-identity-access-management-equals-security-breaches/#Your-Expensive-Cybersecurity-is-only-as-Strong-as-Your-Identity-Access-Management

Vo, T. H., Fuhrmann, W., & Fischer-Hellmann, K.-P. (2017). How to Adapt Authentication and Authorization Infrastructure of Applications for the Cloud. 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud). doi: 10.1109/ficloud.2017.14

Vo, T. H., Fuhrmann, W., Fischer-Hellmann, K.-P., & Furnell, S. (2019). Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment. Future Internet, 11(5), 116. doi: 10.3390/fi11050116

Waltermire, Karen, Burgin, Kelley, Chinedum, Perper, Devin. (2019, June 17). [Project Description] Continuous Monitoring for IT Infrastructure: Techniques for auditing user activity and detecting irregular activity events within small and medium-sized businesses

(Draft). Retrieved from https://csrc.nist.gov/publications/detail/white-paper/2019/06/17/continuous-monitoring-for-it-infrastructure-for-smb/draft.

Weingartner, R., & Westphall, C. M. (2017). A Design Towards Personally Identifiable Information Control and Awareness in OpenID Connect Identity Providers. 2017 IEEE International Conference on Computer and Information Technology (CIT). doi: 10.1109/cit.2017.30

Werner, J., Westphall, C. M., & Westphall, C. B. (2017). Cloud identity management: A survey on privacy strategies. Computer Networks, 122, 29–42. doi: 10.1016/j.comnet.2017.04.030

Winder, D. (2019, August 20). Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019. Retrieved from https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#61cbbcbdbd54

Zefferer, T., Ziegler, D., & Reiter, A. (2017). Best of two worlds: Secure cloud federations meet eIDAS. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). doi: 10.23919/icitst.2017.8356430

Zwattendorfer, B., & Slamanig, D. (2016). The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality. Journal of Information Security and Applications, 27-28, 35–53. doi: 10.1016/j.jisa.2015.11.004

Zwattendorfer, B., Zefferer, T., & Stranacher, K. (2014). An Overview of Cloud Identity Management-Models. Proceedings of the 10th International Conference on Web Information Systems and Technologies. doi: 10.5220/0004946400820092

APPENDIX A

Table A1

Major data breaches

Entity	Year	Records compromised	Organization type	What was exposed	What caused the exposure
Adobe Inc	2019	7.5 million	Technology	User emails, member id, payment details	Misconfiguration of Creative cloud prototype environment, which let to exposed user details on the web, resulting in unauthorized access without a password
Capital One	2019	106 million	Financial	User details such as SSN, customer credit scores, credit limits, balances, payment history, and contact information	Infiltration by third party CSP, exploiting the misconfigured web application firewall to gain access to information
Desjardins	2019	2.9 million	Financial	User details such as SSN, address, phone number, email address and details about banking habits	Insider data theft, poor access control and misuse of data
Facebook	2019	540 million	Social network	exposed 146 gigabytes of Facebook user data, including account names, IDs and details about comments and reactions to posts	Publicly exposed on Amazon's cloud server due to poor security
Biostar2	2019	28 million	Technology	Fingerprint data, facial recognition data, face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, personal details of staff.	The unprotected and unencrypted database was discovered, caused by manipulation of the URL used with elastic search allowed them to access the data.
American medical collection agency	2019	20 million	Healthcare	Social Security numbers, dates of birth, payment card data, and credit card information	Unauthorized user access to a patient's personal and financial information

Note: Norton's Data Breaches report, 2019

Appendix B

Concepts of identity and access management systems

a. Layers of the IAM system

Cloud admins and cloud service customers require an access management interface to manage access to the resources. The access management becomes more complex than the traditional IAM infrastructure since cloud computing is not bound to a single geographic location which draws attention to many risks and threats. An efficient cloud IAM system has the following components. They are 1. User Management (provisioning and deprovisioning), 2. Authentication, 3. Authorization, 4. Access Management and 5. Monitoring & Audit. The IAM life cycle is summarized in the below Figure B1

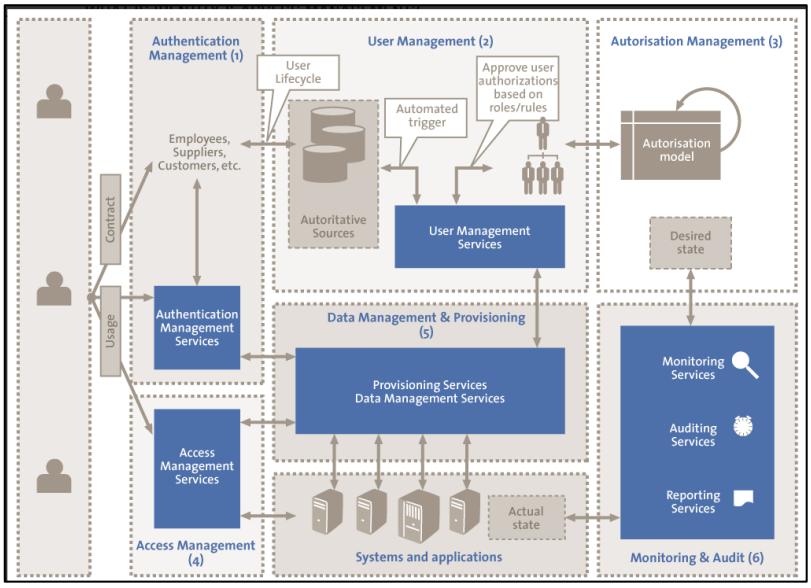

Figure B1. Enterprise IAM reference architecture. Source: Mather, Kumaraswamy & Latif, 2009

User Management: The cloud service customer and the cloud provider agree who is responsible for creating, modification, assigning permissions, role change, deletion and governing all the policies required for administering the lifecycle of the users.

Authentication management: The process of proving the identity of the person, who he claims to be, using various proofing mechanisms such as password, OTP and MFA, biometric, etc.

Authorization management: Authorization is the process of limiting access to the users or groups to that application they can. In the cloud, authorization management follows strict rules which allow the least privilege and segregation of duties. For cloud systems, centralized authorization is introduced, which has more fine-grained authorization rules to manage the access, where the responsibility gets divided between the applications managed and the centralized authorization system.

Access Management: Deals with the access permissions that need to be granted to the users in accessing different cloud services, across the cloud stack (IaaS, PaaS, SaaS) effectively

Provisioning and data management: Deals with the assigning of roles to users when accessing different cloud services., as its roles and permissions are different for each cloud service. The user and their roles are also removed respectively when the employee leaves the organization or subscription has expired. The provisioning is done by just-in-time or on-demand provision via Service Provisioning Markup Language (SPML) or Security Assertion Markup Language (SAML).

Monitoring and Audit Management: Deals with the compliance of policies and security controls that are followed in the IAM lifecycle

Appendix C

Federation protocols and technologies

a. Identity federation specifications classification

The specifications and standards of the identity federations are categorized as web-based and non-web based on the protocols used to exchange the messages. (Carretero et al., 2018).This is represented in Figure C1.

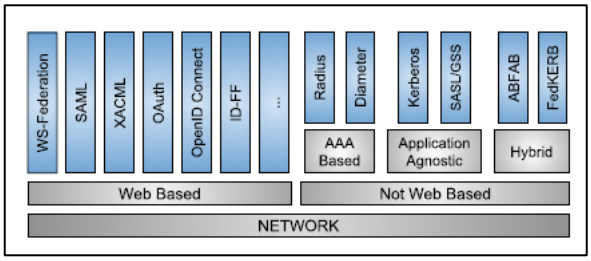

Figure C1. Federation specification. Source: Carretero et al., 2018

1. **SAML:** The Security Assertion Markup Language (SAML) is an open standard for Single Sign-On assertion, used for exchanging authentication and authorization data between Identity providers and service providers. It is an XML oriented framework containing Authentication information, determining the users are who they claim to be; and authorization information, determining the users have the right to access certain systems or content. SAML is used for SSO and attribute-based authentication. The attributes transferred between the SP and IDP are in the form of assertions sending authentication and authorization requests, where the user has no control over the data that is shared from IDP to SP (SAMLV2.0, 2005).
2. **OAuth 2.0:** OAuth is an authorization and delegation protocol, which allows a user to authorize an application or perform some task on behalf of the user. Access to authorized services on the server is controlled using an authorization token. OAuth 2.0 framework

enables a third-party application to gain limited access to the user's resources, without the need for user credentials.

3. **OpenID Connect:** Open ID Connect is an open standard federation identity management model that is adopted by more than one billion OpenID enabled user identities. OpenID Connect 1.0 is developed by adding another identity layer on the top of the OAuth 2.0 protocol. Open ID supports optional features, such as encryption of identity data, the discovery of OpenID Providers, and session management. The information shared between the IDP and SP are self-asserted and rely on federation trust and there is no automated mechanism to verify if either the information exchanged by the SP or IDP is correct.
4. **XACML:** XACML stands for "eXtensible Access Control Markup Language", an international standard for access control policies to achieve interoperability between access control implementations by multiple vendors. XACML is an attribute-based access control system with four major entities policy administration point (PAP), defining policies Policy Decision Point (PDP), that evaluates applicable policy, match requests against policies, and renders an authorization decision; Policy Enforcement Point (PEP), performing access control; And Policy Information and Retrieval Point (PIP), to get and to store access authorization policies and attribute values. The user requests access to PEP, which ask the PDP for the attributes. PDP applies the policy set by the PAP and returns the attributes, which are consulted with the PIP and combined with contextual information to create the obligations to be enforced by the PEP. The architecture is complemented with an attribute-based access control policy language and a processing model to execute policy rules.

b. Other Specifications and Protocols

1. **Liberty Identity Federation Framework: (ID-FF)** was one of the first approaches for identity federation emerging as a consortium of companies from different domains like telecommunication, banks, universities. This framework supports authentication, identity federation, use of pseudonyms, support for anonymity and global logout. Though it is a complete framework, it is not widely adopted but has been included in the Kantara Initiative (Global initiative for innovation for the digital identity transformation that includes identity relation management, user-managed access, and IoT)
2. **Microsoft U-Prove:** U-Prove is a user-centric anonymous credential system developed by Microsoft using claims-based identity management. It uses a U-Prove token, where the prover applies the token private key to a message for verification. It is interoperable as well as unlinkable to users to avoid tracking and allows selective disclosure of user attributes
3. **Idemix:** Idemix is an anonymous credential system designed by IBM. Selective disclosure, unlinkable pseudonyms, and anonymization with claims-based authentication features of Idemix technology has made it be adopted in different European projects like ABC4Trust and Primelife
4. **Shibboleth**: Shibboleth is an open-source SAML implementation allowing authentication, authorization, content personalization, and enables single sign-on across for different providers. Shibboleth is widely used in academic organizations and has an HTTP based SSO approach, where each organization can use a different authentication mechanism.

Appendix D

Large scale identity federation

The large-scale and cross border identity federations like eduGAIN, InCommon, Credential, European, adopt the best in class technologies and combination of protocols by developing, testing and showcasing innovative cloud-based services to the community.

1. **eduGAIN:** eduGAIN is an international federation service connecting research communities and higher education identity federations around the world by linking 5,500 identity providers accessing services from more than 1,700 service providers. It has been developed and operated by GEANT and REFEDS under a series of projects financed by the European Commission, and it uses SAML protocol and the Interoperable SAML 2.0 Profile Currently, eduGAIN has been extended to provide inter-federation services, making it the largest inter-federation service in operation.
2. **InCommon:** InCommon is a US-based research foundation facilitating shared management of access to online resources. InCommon consortium leveraging multiple technologies like Microsoft and Cirrus Identity, and Shibboleth and SAML integration It uses SAML protocol and very similar to the eduGAIN in its features and served 10 million end-users in 2016. Examples of other large-scale identity federation are CLARIN Federated Identity for language resources and technology, DARIAH Authentication and Authorization Infrastructure for arts and humanities, and ELIXIR Authentication and Authorization services for life sciences serving the academia domain.
3. **Credential:** CREDENTIAL is an EU funded research project developing, testing and showcasing innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher

level of security than other current solutions. The main idea and ambition of CREDENTIAL are to enable end-to-end security and improved privacy in cloud identity management services for managing secure access control. This is achieved by advancing novel cryptographic technologies and improving strong authentication mechanisms and secure handling of identity data in high assurance domains like e-Government, e-Health, and e-Business and establishes various use cases for the three domains.

4. **European EID:** Alongside many EU countries German nPA, the Dutch DigiD or the Spanish eDNI, developing their eIdentification systems for their nationals, pan-European eID interoperability infrastructure was developed, allowing cross-border identification using national Ids. This user-centric system enables smooth interaction between citizens and public authorities in Europe by establishing a trusted network. The infrastructure is based on SAML2.0, where each Service provider is connected to the eIDAS node (electronic IDentification, Authentication and trust Services) working in two operation modes, the role of requesting cross border authentication and another in a charge of providing cross border authentication. Similar projects like STORK and STORK 2.0 used PAN European proxy service (PEPS) acting as a single gateway and intermediary for foreign eIDs towards domestic Service providers. The proposal and results were adopted under Regulation (EU) 910/2014 called the eIDAS Regulation, which ensures that people and businesses can use their national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. As a result, it creates a European level trust network on electronic services (e.g. digital signatures) by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.