Defining Cloud Identity Security and Privacy Issues: A Delphi Method

Completed Research

Eghbal Ghazizadeh
AUT University
eghbal.ghazi@aut.ac.nz

Brian Cusack
AUT University
brian.cusack@aut.ac.nz

Abstract

The purpose of this study is to identify the potential security and privacy issues for the entities providing cloud identity services known as cloud identity providers. We document the key security and privacy issues and problems that arise when users and service providers co-operate for cloud service utility. The Delphi method is adopted to facilitate identifying the security and privacy issues in the cloud identity environment. The benefit of using the Delphi method is identification of the issues and prioritizing the relative importance of these issues. A four-round modified Delphi process was applied to a general database of security literature, and then the most relevant articles selected for further analysis. The analysis highlights key issues, advantages and disadvantages of the identity and access management methods; and, risk mitigation mechanisms for identity theft.

Keywords

Cloud Computing, Cloud Identity, Identity and Access Management, Delphi Method.

Introduction

Secure Identity management systems (Gerhart & Sidorova, 2017; Werner, Westphall, & Westphall, 2017) are of paramount importance in providing authentication and authorization based on end-user identities. The challenge is to preserve privacy (Sun, Strang, & Pambel, 2018), while at the same time enhancing interoperability across multiple domains. Traditional identity management systems (Crossler & Posey, 2017) allow end users, to some extent, to manage their personal information for accessing some services. However, Cloud Computing (CC) (Y.-C. Lee, 2019) brings a different perspective related to the end users' interests. New risks arise (Ruiz & Pedraza, 2016), especially due to the fact that the number of devices acting in the system grows exponentially. In this regard, some attacks are more dangerous, and the number of malware types and malicious users has a similar growth pattern. In a network environment, the client authenticates the server and vice-versa. In this way, network users can be assured that they are doing business exclusively with legitimate entities and servers can be certain that all would-be users are attempting to gain access for legitimate purposes. Mutual authentication is gaining acceptance as a tool that can minimize the risk of online fraud in e-commerce. Nevertheless, CC (Zhang, 2018) brings a different perspective related to the end users' interests, which results in new risks (Cayirci & de Oliveira, 2018) for end-user identities. Additionally, end users are more concerned about how their data is managed, where it is located and who can access it. In this sense, CC (Changchit & Chuchuen, 2018) is changing some of the basic assumptions around information management.

Due to the user-centricity and privacy-preserving (Strang & Pambel, 2018; Sun et al., 2018) features offered by identity management systems, these are becoming a key element in CC environments (Tormo, Mármol, & Pérez, 2014). Cloud computing integrates technologies and concepts from other fields, such as multi-party computation, distributed systems, and federation. Therefore, some of the raised challenges are already resolved in other contexts, where identity management systems have been widely accepted. Nevertheless, CC brings a different perspective in which multiple technologies and services require end user identities. Identity management systems are exposed to a number of threats that can compromise their behavior when malicious users or entities try to subvert the system. Identity management systems (Werner

et al., 2017) are aimed to simplify the end user experience but create considerable trust complexity for both service providers and identity providers. They require an infrastructure where all the involved parties must be trusted for specific purposes depending on their role. However, if one of the parties acts maliciously, then the remainder of the participants are exposed to unplanned risks. Identity and Access Management (IAM) systems need to deploy mechanisms to allow entities to trust each other although in some scenarios the trust conditions can introduce threats if risk mitigation mechanisms are not in place. This paper is structured to review identity management systems, to locate the cloud identity security (Tari, Yi, Premarathne, Bertok, & Khalil, 2015) and privacy issues, the required trust factors, and to structure a risk framework for the management of privacy issues. The paper explores security and privacy issues (Werner et al., 2017) that are the key to building consumer trust in Cloud services. The communication of trustworthiness to create positive expectations and thus influence consumer intentions and behavior are key to trust formation. The Delphi method (El-Gazzar, Hustad, & Olsen, 2016; Lynn, Van Der Werff, Hunt, & Healy, 2016), is used in the cloud IAM context to locate the important features of CC services, transparency elements and perceptions of trustworthiness. The Delphi method is applied to analyze research papers and to define a complex problem for a consensus analysis through a series of rounds. The purpose of this paper is to define the cloud identity security and privacy issues and to clarify the current related problems.

Delphi Method

Based on the Delphi method (El-Gazzar et al., 2016; Fowler & Dyer, 2018; Lynn et al., 2016), this study focuses on the most important issues enterprises are confronting with CC and cloud identity. However, while there are studies that have focused on technological aspects regarding cloud and cloud identity, the decision regarding whether to adopt and migrate to CC solutions is additionally complicated by privacy (Nuñez, Agudo, & Lopez, 2015) and security issues (Nagaraju & Parthiban, 2015). Several types of research approach (Ruiz & Pedraza, 2016; Strang & Pambel, 2018; Sun et al., 2018) have identified that there is a lack of empirical evidence and knowledge regarding which issues have the biggest impact on security and privacy. This study reviews the current literature, and consequently fills a gap by identifying the most important issues related to CC and cloud identity adoption decisions in enterprises. The relative significance of the identified issues is determined, and the importance ranked.

In this regard, we found that the Delphi method is one of the best ways to identify and prioritise issues for decision making and to sort large volumes of references. The Delphi Method assists in identifying the research questions and issues associated with the research topic. To facilitate the research processes first questions were selected to focus the target, and used to guide the collection of relevant literature, as follows:

"Q1: What issues confront entities when adopting CC and cloud identity?

Q2: What is the relative importance of these issues?

Q3: Why are these issues important?"

The literature contains a selection of academic literature related to CC and cloud identity. Therefore, identifying the most relevant challenges, approaches, issues, and techniques in the research scope is the objective. As a result, the method is applied to identify the relevant literature as shown in figure 1. The main objective of the Delphi method is to systematically seek the most reliable opinion from a group of possibilities (research papers) that are usually experts (author(s)) or selected groups within the scope of the research. The Delphi method has an established reputation in Information Systems (IS) studies as a tool and a methodology to justify literature selection. It is known to be a qualitative research technique with quantitative elements (Gonzalez et al., 2012). We found the method helpful to process the large amount of general literature available in the topic scope and to select the relevant literature. The iterative rounds refine the target to a point the required themes become clear and the volumes of information manageable.

Delphi as a research methodology has been variously presented as a literature review and survey procedure, method, and technique. In this paper, we refer to Delphi as a 'method' because this appears to be the most commonly used terminology in the research literature. Nowadays, it is a popular way of engaging opinion from the different points of view and different researchers, although, the method itself and the purposes for which it has been used have been extensively modified by researchers over the years. Hence, in this paper,

the Delphi method is the guideline and methodology to identify the most common security and privacy issues related to the cloud identity environment.

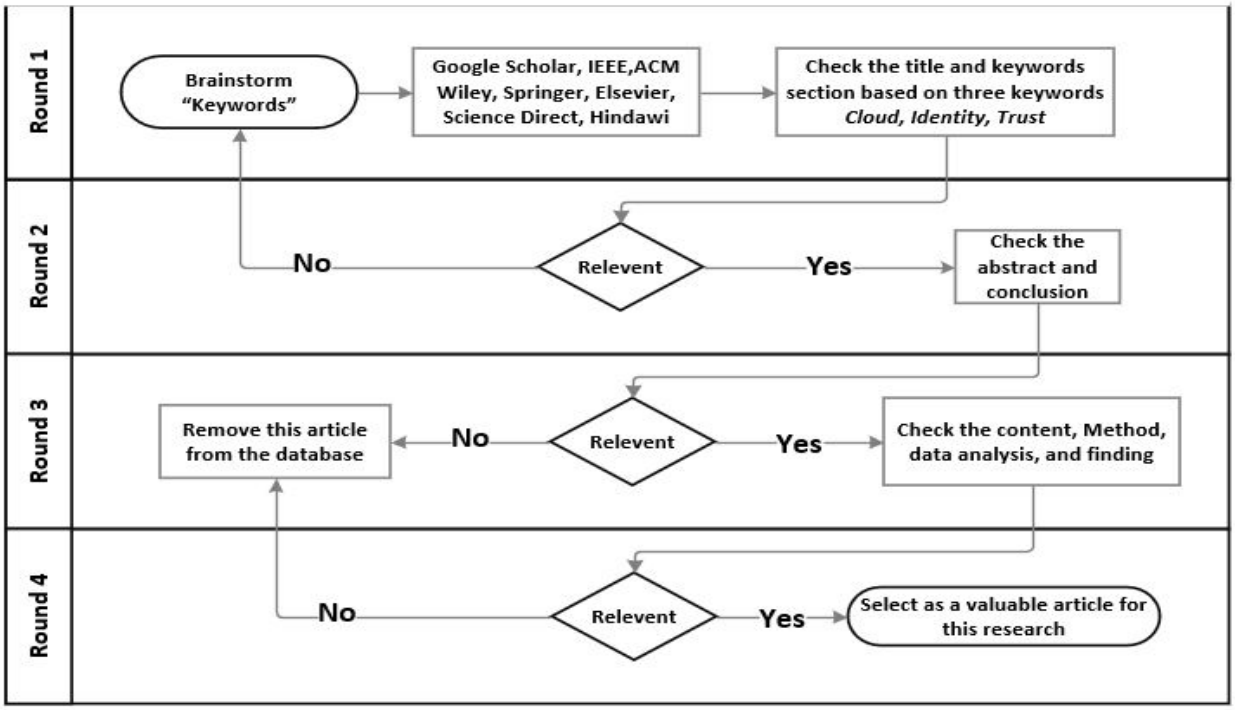

Figure 1. Delphi Technique

Define Method Applications

This section outlines the adoption of the Delphi method. Therefore, in round 1, the question is: "What are the issues that enterprises confront when adopting CC services, cloud identity, and trust computing?" A digital library search (IEEE, Google Scholar, Science Direct, Elsevier, Springer, ACM, Hindawi, and Springer) was undertaken to provide issues, as well as to define each issue, justify its importance and consequences, and if possible, add comments for elaboration. Given the diversity of topics in the millions of academic papers, the research method assists in finding the most relevant papers. Therefore, the following steps identify the processes involved and the paper selection criteria. The CC, Cloud identity, Cloud issues and federated identity issues are used as keywords to search in the title on the eight selected databases. The selected papers are limited between the year 2001 to the year 2019 (the most recent at the time of the research). The next step is to check the quality of the papers based on their abstract and conclusion, and relevancy to the search questions. Consequently, checking the content of the papers, which passed the previous step, leads to the final round where the papers are selected. The benefit of using the Delphi method is that it allows the researcher to focus on the research problem. Also, to systematically gather the latest and up to date, scholarly papers is another advantage (El-Gazzar et al., 2016; Fowler & Dyer, 2018; Lynn et al., 2016).

Cloud Evolving Challenges

One of most effective methods to overcome security and privacy issues of providing public and private cloud between Cloud Service Customers (CSC) and Cloud Service Providers (CSP) is advanced identity and access management (Nuñez & Agudo, 2014; Werner et al., 2017). The system provides benefits for all those in roles responsible for providing secure access to cloud resources and to those who want to outsource or create online services. The provision of secure identity management is one of the best methods to overcome the security concerns of CC security issues. However, IAM provides authentication and authorisation based on CSC' identities in order to preserve security and privacy, while at the same time enhancing interoperability

across numerous identities. After four rounds of the Delphi method, the analysis of the research papers shows the main objective for IAM in the cloud is to bring a different perspective related to the CSC interests.

In order to gain an acceptable security level in the cloud, a CSP has to understand and achieve the privacy and security requirements of their customers. Therefore, finding and identifying a common understanding and conceptual foundation of the CSC is crucial for CSP satisfaction. The Delphi method delivers these answers and consequently the challenges. The process requires integration of the Delphi method with technical known and unknown requirements, technologies and implementation capability. The research showed that common challenges for the CC are:

- *The contrast between public and private clouds*: Where several security issues provide evidence to stay in private clouds.
- *Outsourcing storage and computing:* Where the CSPs offer a complete set of characteristics that embrace all cloud requirements, such as public verifiability.
- *Virtualised:* Where virtualisation still is a complex area of cloud with virtual resources, and isolates running components.
- *Malware:* Where Cloud Malware in CC is commonly used by the CSCs.
- *Web-based technologies:* There is a wide attack vector associated with delivering applications over the Internet
- *Networking perimeter:* Where the security overlay for network design assumes a secure cloud environment.
- *Trust:* Is a barrier that transversely extends throughout the whole of cloud components and stakeholders.
- *Privacy:* Where there is an increasing government desire to mass supervise data from CSCs in the scope of general data protection policies.
- *Standardise:* This aims to speed up the migration of current cloud environments to interoperable and standardised cloud systems.

Privacy, Theft and Attack

It is vital to update and synchronised identity information (Arbore, Soscia, & Bagozzi, 2014) to avoid any conflicts caused by the usage of on-premise user data. Therefore, in terms of privacy, it is very important to choose a secure IAM that best supports the CSC's privacy requirements because IAM is exposed to threats that can compromise CSP's behaviour when malicious users or entities try to subvert the system (Tormo, Millán, & Pérez, 2013). Furthermore, privacy is a desired feature both CSCs and CSPs, therefore, CSCs seek to keep secret the information of their digital identities, as well as CSPs, have to deploy mechanisms to preserve CSC' privacy. In this regard, CSPs seek to align with anonymity which means they cannot know the real identity of CSCs, unlinkability, which means a CSPs cannot link different CSC's accesses. The analysis based on the result of the Delphi method shows that with anonymity as a privacy characteristic, un-traceability is also another privacy issue which means Cloud Identity Providers (CIdP) cannot know the services that one of its end users has accessed (Shaikh & Sasikumar, 2013).

According to (Gerhart & Sidorova, 2017), the definition of identity theft is the exploitation of other user's individual information to perform fraud. The Delphi method identified the research related to identity theft. Account fraud is one of the subcategories of identity theft. In the account, fraud an attacker takes advantage of existing accounts, and they make a new action based on the victim account. Moreover, there are two ways for common identity theft: Diving rooting through garbage for personal information is the first and a low-technology method. Hacking into collective computer systems is the second and high-tech method. The attackers steal a laptop including identity information, or they do Phishing attacks and exploit malicious computer code to get the user or system information. Also, weak cryptography between identity provider, users, and service providers is one of the reasons for identity theft.

Currently, many research articles (Jensen, 2013; Mahalle, Anggorojati, Prasad, & Prasad, 2013) are focused on cloud IAM, while, security and privacy of IAM in the cloud are aspects that are still in development stages and require further exploration. The selected papers from four rounds of Delphi method shows that current IAMs are susceptible to various security and performance bottlenecks, which limits their federation adoption as a potential solution for the federation cloud. Therefore, Cloud-based IAM and security issues are relevant. The detailed analysis of the selected papers shows that the following attacks are the most common attacks in the area of cloud identity:

- Brute-force attack: Where unauthorised access by an attacker to sensitive identity credentials of CSCs stored in CIdPs' server using diverse methods to get the ID and password as in a dictionary attack (J.-K. Lee, Kim, Woo, & Park, 2015).
- Cookie-replay attack: The attacker steals a cookie containing valid session information along with the identity credential of the CSC (Rakotondravony et al., 2017).
- Data Tampering Attack: Where the manipulation of the identification of CSC in an identity data-store at CIdPs (Mun & Han, 2016).
- Denial of Service (DOS) Attack: Refers to non-availability of the CIdPs due to false authentication or authorisation which has been requested by attackers (Nor & Jalil, 2012).
- Eavesdropping: Refers to getting access to the identity credentials by attackers while both CIdP and Cloud Identity Users (CIdU) are exchanging the credential (Khorshed, Ali, & Wasimi, 2012).
- Elevation of Privilege: Refers to the escalation of the privilege by attackers in order to achieve their illegal objectives and may cause severe damage to the CSC' information (da Costa Cordeiro, Santos, Mauch, Barcelos, & Gaspary, 2012).
- Identity Forgery/Cloning/Spoofing Attack: Refers to the ability of manipulation or copying identity tokens by the attackers (Huang, Ma, & Chen, 2011).
- Identity Theft: Identity theft means that attackers can steal the CSC's identity, with the intent to acquire CSP' resources (Callegati, Cerroni, & Ramilli, 2009).
- Phishing Attack: In this attack, the attackers seek to acquire CSC's information such as social security number, name, passwords, and credit card details by redirecting the CSC to enter a fake environment (Rakotondravony et al., 2017).
- Repudiation: Refers to a lack of maintaining CSC's activity log so no proof exists to prove accountability for actions (Duncan, Creese, & Goldsmith, 2015).
- Side-Channel Attack: Refers the stealing the identity information from the physical implementation by the attackers (Zhou, Goel, Desnoyers, & Sundaram, 2013).
- Skimming Attack: In this method, the attackers steal sensitive information from authentication tokens such as smart cards (Gruschka & Jensen, 2010).
- Snooping attack: Refers to the techniques to gather victim information through surveillance methods such as key-loggers monitoring through remote activity (Habiba, Masood, Shibli, & Niazi, 2014).
- Sybil attack: Where the attackers are subverting the reputation of either CSPs or CIdPs (Habiba et al., 2014).
- Whitewashing attack: Where the attackers reset weak reputation levels of either CSPs or CIdPs (Habiba et al., 2014)
- False praise attack: Where the attackers give more weight to the past reputation levels of either CSPs or CIdPs (Habiba et al., 2014)

System Access

The most common identity management technologies and solutions to manage the end user's attributes provide system access (Balamurugan & Krishna, 2015; Seltsikas & O'keefe, 2010; Spencer, 2012). The advantages and disadvantages of the system access are highlighted in regard to the cloud identity system access (Y.-C. Lee, 2019). This analysis is based on the selected paper from the round four Delphi method. The first cloud IAM is OpenID which is a part of the Single Sign-On (SSO) (Chadwick, Casenove, & Siu, 2013; Méndez, López, & Millán, 2016). It is commonly used by CSPs for exchanging their identity. Also, it is based on the Security Assertion Markup Language (SAML) protocol (Lutz & Stiller, 2013) which is determined by the same requirements for web SSO, but the design goal is different (Mahalle et al., 2013). The main idea is that a user can authenticate by URL and then exhibit their preferred OpenID Provider (Bilal, Asif, & Bashir, 2018). Another cloud IAM is OAuth which defines a protocol in order for clients to access server resources on behalf of a resource owner. It provides a process for end-users to authorise third-party accesses to their server resources without sharing their credentials. Windows CardSpace or InfoCard is the system which has been designed by Microsoft for identity selection. It allows the end users to align with an identity lifecycle and create, use, and manage their identities. The main design purpose is to manage the digital identities, and the user's attributes in a similar way as to manage a wallet's cards. Also, U-Prove is a method that is using cryptography techniques to encode end users' attributes. Utilising the Zero-knowledge methods is the main feature of the issuing the tokens by U-Prove Cloud IAM. Moreover, the Identity Mixer (Idemix) is similar to U-Prove but focuses on privacy, which allows the customers to control the dissemination of personal information in order to enhance user privacy. Likewise, Higgins is designed to integrate the social relationships information and identity profiles with numerous providers to improve the open source identity framework. The OpenID Connect is based on the OAuth 2.0 protocol. It is used to simplify the process of identity management. The capability of these methods is categorised for performance in figure 2, and then analysed in Table 1.

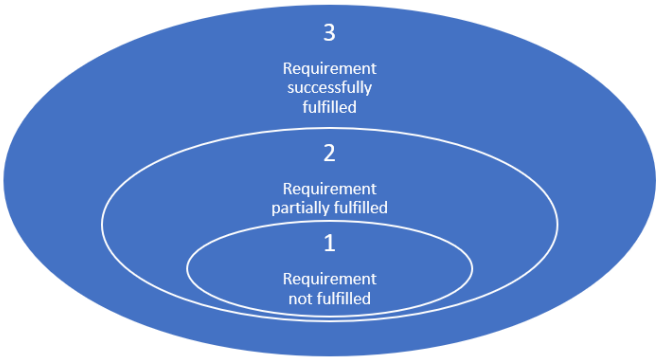

Figure 2. Levels of Requirement Fulfilled

Limitations of IAM Protocols

The literature analysis found that IAM would be efficient and secure by integrating various scenarios and techniques. Therefore, integrating and establishing a trust relationship in addition to security and privacy techniques brings efficiency to the cloud environment (Y.-C. Lee, 2019) as well as offering a large range of features (Sharma, Menard, & Mutchler, 2019; Tormo et al., 2014). The IAM is the key element in CC because it provides identity management for both CSCs and CSPs. Therefore, IAM seeks to integrate various systems such as distributed systems multi-party computation, and federation to achieve this objective. Therefore, while IAM has been widely accepted, nevertheless, CSCs are more concerned about how their identity is managed (Habiba et al., 2014). The detailed analysis of the selected papers based on the Delphi method identified the features and limitations of the common cloud IAM. Also, based on the characteristics (Tormo et al., 2014), we grouped these identity management systems based on their requirement in three main categories: General requirements, User-centric capabilities, and Information management functionalities as shown in figure 3. Also, we have found that there is no ideal cloud IAM fulfilling all the requirements. As the main contribution for this research paper, we summarized the results in figure 3 and table 1 to indicate the level of requirement fulfilled. Table 1 illustrates the current level of security and privacy and their overall

weight based on the technical features. This structure is a method to measure the strengths and weaknesses of the Cloud IAM standards.

Discussion

Privacy is a coveted element of any correspondence system. However, CSCs desire to secretly store their identity and information, but, on the other hand, the CSPs need to know the information about their customers. Though some CSPs do not need to know the real identities of their customers, they do require to gather the most relevant information. Therefore, to fulfill both providers and customers expectation, IAM have to preserve customers' privacy by implementing strong privacy methods which provide anonymity (lack of the knowing real identity of the CSCs by the CSPs), unlikability (lack of link between numerous CSCs accesses by the CSPs), and intractability (lack of knowing the services which have been accessed by the CSCs).

Moreover, new policies by policymakers, the concept of fairness, and requirements by law (Haley et al., 2017; Nicolaidou & Georgiades, 2017) are leading to changes in regards to privacy for individuals compared with the common pragmatic approach for free speech. The draft US Privacy Bill of Rights (Parker, 2017) and the EU General Data Protection Regulation (GDPR) are two examples of changes to privacy concerns. Moreover, these documents offer numerous and crucial changes for CSPs that need to meet various global privacy regulations. Trans-border data flow restrictions and geographic regulation are the two most common privacy issues for the CC environments. The analysis of the privacy issues in this research showed that a lack of user control, lack of training and expertise, unauthorized security usage, complexities in regulatory compliance, trans-border data flow restrictors, and legislation are common privacy issues which have been shown in previous sections. Table 1 presents a summary of findings.

Category	Code	Essential functionality/ requirements/operation	OpenID	SAML	OAuth	CardSpace	Higgins	UProve	Idemix
General requirements	R1	Confidentiality and integrity	3	3	3	3	3	3	3
	R2	Single Sign-On	3	3	3	3	3	3	3
	R3	Logging and Auditing	3	3	2	3	3	1	1
	R4	Strong authentication	2	2	1	3	3	3	3
	R5	Justifiable parties	1	2	3	2	2	2	2
User-centric capabilities	R6	End user consent	3	1	1	3	3	3	3
	R7	Control of accumulated data	1	1	3	3	3	3	3
	R8	Usability	3	3	3	2	2	1	1
Information management functionalities	R9	Off-line mode	1	1	3	1	3	1	1
	R10	Attribute aggregation	1	1	1	1	1	1	1
	R11	Attribute revocation	3	3	2	2	2	1	1
	R12	Self-asserted attributes	2	1	2	3	3	3	3
	R13	Minimal disclosure information	3	1	2	2	2	1	1
Overall			29	25	29	31	33	26	26
Average			2.2	1.92	2.23	2.38	2.54	2	2

Table 1. Comparison of Current IAM Solutions

CSP have the same requirements as any computation system. It is exposed to various security risks that can compromise the security of the system. Attackers by utilizing malicious intents with novel methods are trying to attack any service provider by knowledge and enumeration methods. The security issues are crucial for CIdPs because they manage CSC's sensitive data (digital identity). Therefore, in responding to security issues, IAMs need to provide a secure system to protect digital identities and mitigate identity theft.

Based on the most relevant papers (Round 4 Delphi method), there are different attacks and security vulnerabilities for both CSPs and CIdPs. Some of them are coming from traditional computing, but some of them are new. These attacks need new methods and research to mitigate threats (Sethi & Sruti, 2018). As a summary for the security issues (figure 3) the authors found that unwanted access, vendor lock-in, inadequate data deletion, compromise of the management interface, backup vulnerabilities, isolation failure, missing assurance and transparency, inadequate monitoring, inadequate compliance, and inadequate audit are the most common issues.

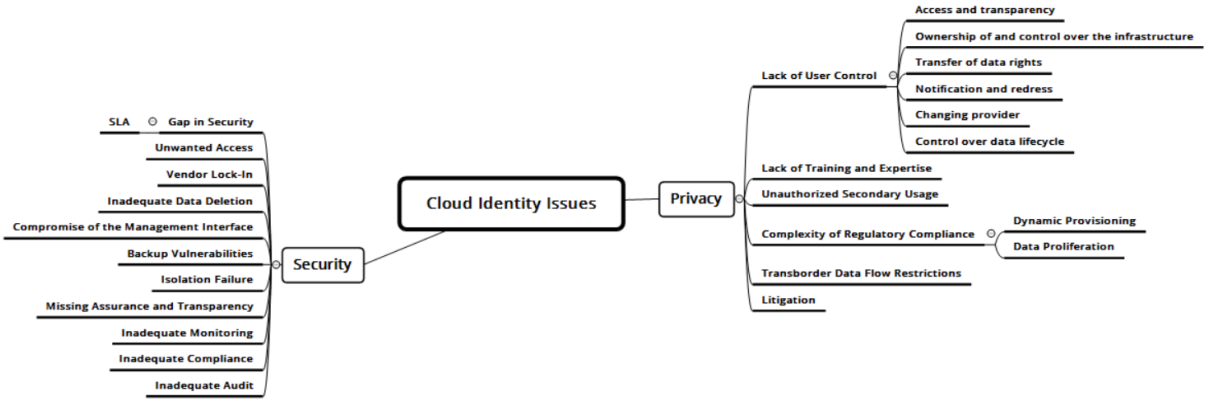

Figure 3. Cloud Identity Security and Privacy Issues

Conclusion

In CC, end users are more concerned about how their data is managed, where it is located and who can access it. In this sense, CC is changing some of the basic assumptions regarding data protection. As a result, any service in the cloud is exposed to trust, security and privacy threats that can compromise the identity of end users. The literature analysis completed found the different identity management approaches each address different issues and CC problem areas. The questions left open regard the fit of these proposals in the evolving CC environment. We also provide a set of recommendations to be taken into consideration when designing or deploying any identity-based service in a cloud environment. In particular, the evolving state of privacy issues is not yet well represented in current security designs. There is an ongoing change in privacy requirements, and it is the biggest requirement shift since the nineteen eighties. Efforts are being put in fairness, accountability and increased protection by policymakers. There is an increasing government desire to supervise data from Internet users for cyber threat protection. Although the ultimate goal is to actively prevent or mitigate cyber threats, Identity management systems have been proved to be sufficiently secure and efficient in diverse contexts and scenarios. By establishing trust relationships between providers and domains, identity management systems offer a huge range of features both for end users and for organizations regarding controlling and exchanging identity-related information in a privacy-aware way.

This research is focused on identifying contemporary security and privacy issues in the cloud identity environment. The Delphi method employed in this study relied on the most relevant research papers selected for the analysis. The findings indicate that the researchers meet a number of evaluation criteria (general requirement, user-centric capabilities, and information management functionalities), but the CIdPs have yet to be tested. The limitation this presents is that a low number publications concern the CIdU in the wider consumer population. Future research including expert contribution is required to investigate the security and privacy of the CC. A wider population would also allow investigation of the security and privacy impact of personal variables on trustworthiness perceptions in the CC environment. Future research can also examine how perceptions and understanding of the information in the CC affects security design. These factors can influence consumer attitudes, decision making based on security, and privacy attributes. Thus, analysis of the CIdP's capabilities from the perspectives of general requirements, user-centric capabilities, and information management functionalities, may inform different services, risk levels, and service provider awareness.

Acknowledgements

Hanif Deylami is acknowledged for editorial help and literature identification for this paper.

REFERENCES

Arbore, A., Soscia, I., & Bagozzi, R. P. 2014. "The Role of Signaling Identity in the Adoption of Personal Technologies," *Journal of the Association for Information Systems, (15:*2), p. 86.

Balamurugan, B., & Krishna, P. V. 2015. "Enhanced Role-Based Access Control for Cloud Security," *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems,* pp. 837-852.

Bilal, M., Asif, M., & Bashir, A. 2018. "Assessment of Secure OpenID-Based DAAA Protocol for Avoiding Session Hijacking in Web Applications," *Security and Communication Networks, (20:1), p. 8.*

Callegati, F., Cerroni, W., & Ramilli, M. 2009. "Man-in-the-Middle Attack to the HTTPS Protocol," *IEEE Security and Privacy, (7:*1), pp. 78-81.

Cayirci, E., & de Oliveira, A. S. 2018. "Modelling trust and risk for cloud services," *Journal of Cloud Computing, (7:*1), p. 14.

Chadwick, D. W., Casenove, M., & Siu, K. 2013. "My private cloud–granting federated access to cloud resources," *Journal of Cloud Computing: Advances, Systems and Applications, (2:*1), p. 3.

Changchit, C., & Chuchuen, C. 2018. "Cloud computing: an examination of factors impacting users' adoption," *Journal of Computer Information Systems, (58:*1), pp. 1-9.

Crossler, R. E., & Posey, C. 2017. "Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem," *Journal of the Association for Information Systems, (18:*7), p. 487.

da Costa Cordeiro, W. L., Santos, F. R., Mauch, G. H., Barcelos, M. P., & Gaspary, L. P. 2012. "Identity management based on adaptive puzzles to protect P2P systems from Sybil attacks," *Computer Networks, (56:*11), pp. 2569-2589.

Duncan, A., Creese, S., & Goldsmith, M. 2015. "An overview of insider attacks in cloud computing. *Concurrency and Computation: Practice and Experience," (27:*12), pp. 2964-2981.

El-Gazzar, R., Hustad, E., & Olsen, D. H. 2016. "Understanding cloud computing adoption issues: A Delphi study approach," *Journal of Systems and Software, (118)*, pp. 64-84.

Fowler, K. R., & Dyer, S. A. 2018. "Crowdsourcing Versus Delphi Method," *IEEE Systems Journal.*

Gerhart, N., & Sidorova, A. 2017. "The effect of network characteristics on online identity management practices," *Journal of Computer Information Systems, (57:*3), pp. 229-237.

Gonzalez, N., Miers, C., Redígolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. 2012. "A quantitative analysis of current security concerns and solutions for cloud computing," *Journal of Cloud Computing, (1:*1), pp. 1-18.

Gruschka, N., & Jensen, M. 2010. "*Attack Surfaces: A Taxonomy for Attacks on Cloud Services".* Paper presented at the IEEE CLOUD.

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), pp. 1-37.

Haley, D. F., Vo, L., Parker, K. A., Frew, P. M., Golin, C. E., Amola, O., . . . Lancaster, K. 2017."Qualitative Methodological Approach," *Poverty in the United States,"* pp. 9-23.

Huang, C.-Y., Ma, S.-P., & Chen, K.-T. 2011. "Using one-time passwords to prevent password phishing attacks," *Journal of Network and Computer Applications, (34:*4), pp. 1292-1301.

Jensen, J. 2013. "Identity management lifecycle-exemplifying the need for holistic identity assurance frameworks," *Information and Communication Technology*, pp. 343-352.

Khorshed, M. T., Ali, A. S., & Wasimi, S. A. 2012. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation computer systems, (28:*6), pp. 833-851.

Lee, J.-K., Kim, S.-J., Woo, J., & Park, C. Y. 2015. "Analysis and Response of SSH Brute Force Attacks in Multi-User Computing Environment," *KIPS Transactions on Computer and Communication Systems, (4:*6), pp. 205-212.

Lee, Y.-C. 2019. "Adoption intention of cloud computing at the firm level," *Journal of Computer Information Systems, (59:*1), pp. 61-72.

Lutz, D. J., & Stiller, B. 2013. "A survey of payment approaches for identity federations in focus of the saml technology," *IEEE Communications Surveys & Tutorials, (15:*4), pp. 1979-1999.

Lynn, T., Van Der Werff, L., Hunt, G., & Healy, P. 2016. "Development of a cloud trust label: a Delphi approach," *Journal of Computer Information Systems, (56:*3), pp. 185-193.

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. 2013. "Identity authentication and capability based access control (iacac) for the internet of things," *Journal of Cyber Security and Mobility, (1:*4), pp. 309-348.

Méndez, A. P., López, R. M., & Millán, G. L. 2016. "Providing efficient SSO to cloud service access in AAA-based identity federations," *Future Generation Computer Systems, (58)*, pp. 13-28.

Mun, H.-J., & Han, K.-H. 2016. "Blackhole attack: user identity and password seize attack using honeypot," *Journal of Computer Virology and Hacking Techniques*, pp. 1-6.

Nagaraju, S., & Parthiban, L. 2015. "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," *Journal of Cloud Computing, (4*:1), p. 22.

Nicolaidou, I. L., & Georgiades, C. 2017. *The GDPR: New Horizons EU Internet Law*, pp. 3-18, Cham, Switzerland, Springer.

Nor, F. B. M., & Jalil, K. A. 2012. "Mitigating man-in-the-browser attacks with hardware-based authentication scheme," *International Journal of Cyber-Security and Digital Forensics (IJCSDF), (1:*3), pp. 204-210.

Nuñez, D., & Agudo, I. 2014. "BlindIdM: A privacy-preserving approach for identity management as a service," *International Journal of Information Security, (13:*2), pp. 199-215.

Nuñez, D., Agudo, I., & Lopez, J. 2015. "Privacy-Preserving Identity Management as a Service," *Accountability and Security in the Cloud*, pp. 114-125.

Parker, R. B. 2017. "A definition of privacy *Privacy,"* pp. 83-104.

Rakotondravony, N., Taubmann, B., Mandarawi, W., Weishäupl, E., Xu, P., Kolosnjaji, B., . . . Reiser, H. P. 2017. "Classifying malware attacks in IaaS cloud environments," *Journal of Cloud Computing, (6:*1), p. 26.

Ruiz, M. D. M. L., & Pedraza, J. 2016. "Privacy Risks in Cloud Computing," *Intelligent Agents in Data-intensive Computing,* pp. 163-192.

Seltsikas, P., & O'keefe, R. M. 2010. "Expectations and outcomes in electronic identity management: the role of trust and public value," *European Journal of Information Systems, (19*:1), pp. 93-103.

Sethi, S., & Sruti, S. 2018. "Cloud Security Issues and Challenges," *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications,* (pp. 77-92), Sarang, India: IGI Global.

Shaikh, R., & Sasikumar, M. 2013. "Identity Management in Cloud Computing," *International Journal of Computer Applications, (63), p.* 11.

Sharma, S., Menard, P., & Mutchler, L. A. 2019. "Who to trust? Applying trust to social commerce," *Journal of Computer Information Systems, (59:*1), pp. 32-42.

Spencer, T. 2012. "Identity in the cloud," *Computer Fraud & Security,* (7), pp. 19-20.

Strang, K. D., & Pambel, F. 2018. "Privacy and security in the big data paradigm," *Journal of Computer Information Systems*, pp. 1-10. doi:10.1080/08874417.2017.1418631

Sun, Z., Strang, K. D., & Pambel, F. 2018. "Privacy and security in the big data paradigm," *Journal of Computer Information Systems*, pp. 1-10.

Tari, Z., Yi, X., Premarathne, U. S., Bertok, P., & Khalil, I. 2015. "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges," *Cloud Computing, IEEE, (2:*2), pp. 30-38.

Tormo, G. D., Mármol, F. G., & Pérez, G. M. 2014. "Identity Management in Cloud Systems," *Security, Privacy and Trust in Cloud Systems,* (pp. 177-210), Berlin, Heidelberg: Springer.

Tormo, G. D., Millán, G. L., & Pérez, G. M. 2013. "Definition of an advanced identity management infrastructure," *International Journal of Information Security, (12:*3), pp. 173-200.

Werner, J., Westphall, C. M., & Westphall, C. B. 2017. "Cloud identity management: A survey on privacy strategies," *Computer Networks, (122)*, pp. 29-42.

Zhang, R. 2018. "The impacts of cloud computing architecture on cloud service performance," *Journal of Computer Information Systems*, pp. 1-9.

Zhou, F., Goel, M., Desnoyers, P., & Sundaram, R. 2013. "Scheduler vulnerabilities and coordinated attacks in cloud computing," *Journal of Computer Security, (21:*4), pp. 533-559.